DESIGN AND MANUFACTURING (D&M)

SAFETY MANAGEMENT SYSTEM (SMS)

PILOT PROJECT GUIDE

For:

D&M's SMS
Pilot Project Participants and
Voluntary Implementation of SMS Programs

Federal Aviation Administration

Aircraft Certification Service – MSMS Project

Change and Revisions Log

Revision #	Date	Pages/Section Affected	Description of Revision
-	01/20/11	Initial issue	
A	03/04/11	Section 7.1 Paragraph 6.3.2 Paragraph 6.3.3 Section 8 Section 9 Section 9.3 1) Figure 3 Part C Section 12 Section 14.1 Appendix D	Section deleted New paragraph added Revised to add "with the involvement of the company's Participant Management Team" Section 12 moved to create new Section 8 Point 4) added Point f) added Illustration revised Title added New section added Hazard definition revised Appendix revised
B	04/05/11	All sections	Completed a technical edit on the entire document that refined grammar, acronyms, abbreviations and punctuation. No substantive content changes were made.
C	10/21-11	Various sections Section 4.5.1 Section 5 Section 5.2.4 Section 6.3.4 Section 9 Section 9.3 Various sections Section 11.1	Clarified " entire organization" Revised language for level one outputs Revised exit level language Revised to add "…participant may implement any SMS process and procedure at any time..." Added clarification of responsibilities Added clarification to implementation plan content Aligned outputs with appendix B Removed comment letter Replaced objective evidence language with other terminology Addressed coverage of assessment

		Section 12 Section 14.1 Appendix A Appendix B Appendix D	Added information on oversight process Replaced “rating” with “status” Revised Framework to match align with Part 5 Revised activities, outputs, exit criteria ,etc Added updated System description chart

Table of Contents

Table of Figures

1 Purpose of the Guide

This Design and Manufacturing (D&M) Safety Management System (SMS) Pilot Project Guide will be referred to as "the Guide."

The Guide serves as the primary source of information for participants and Federal Aviation Administration (FAA) entities involved in the FAA Aircraft Certification Service (AIR) D&M SMS Pilot Project.

The overall purpose of the Guide is to assist:

1) D&M organizations in participating in the pilot project and provide general information on how to begin developing and implementing an SMS; and
2) FAA Participant Management Teams (PMTs) in evaluating an organization's SMS program and participating in further development of implementation and oversight strategies.

Specifically, it will help ensure that an organization's SMS will be capable of:

1) Receiving safety input from internal and external sources and integrating that information into their operational processes;
2) Establishing and improving organizational safety policy to the highest level;
3) Identifying, analyzing, assessing, controlling, and mitigating safety hazards;
4) Measuring, assuring, and improving safety management at the highest level;
5) Promoting an improved safety culture throughout the entire* organization; and
6) Improved efficiency and reduced operational risk.

While the Guide does provide general guidance on how the pilot project will be conducted and what participants are expected to do during the pilot project, there are two other accompanying files that provide additional information. It is highly recommended that participants review the following materials:

1) D&M SMS Gap Analysis Tool file – Overview information and instructions are provided on the first tab;

2) Developmental Guidance for Design and Manufacturing Safety Management System Framework - For D&M SMS Pilot Project Participants and Voluntary Implementation of SMS Programs

**Entire organization participating within the scope of the system description*

2 Applicability

The Guide is designed for application by both D&M organizations that desire to develop and implement an SMS.

Developing an SMS – The D&M *SMS Framework* and this Guide apply to aviation D&M organizations that participate in the D&M SMS Pilot Project and to all others who desire to develop and implement an SMS. The D&M *SMS Framework* is not mandatory and does not constitute a regulation. Development and implementation of an SMS is voluntary. While the Federal Aviation Administration (FAA) encourages each aviation D&M organization to develop and implement an SMS, these systems are not substitutes for compliance with Federal regulations and all other certificate requirements, where applicable. However, for aviation D&M organizations that voluntarily implement an SMS, the FAA views the objectives and expectations in this Framework to be the minimum for a comprehensive and robust SMS.

The D&M *SMS Framework* is a functional expectations document. The document stresses what the organization must do to implement a robust SMS rather than how it will be accomplished. At the same time, the Framework needs to be applicable to a wide variety of types and sizes of organizations. Therefore, by design, it is scalable and allows organizations to integrate safety management practices into their unique business models.

3 Recommended Reading Material

The following references are recommended reading material for users of this Guide in the development and implementation of an SMS. All other documents referenced within this document are identified in the page footnotes.

1) *Safety Management Systems for Part 121 Certificate Holders Notice of Proposed Rulemaking (14 CFR Parts 5 and 119, Docket No. FAA–2009–0671) – Federal Register Volume 75, No. 214, page 68242; Friday, November 5, 2010.*

2) *International Civil Aviation Organization (ICAO) SMS Framework – Annex 6 to the Convention on International Civil Aviation, Operation of Aircraft, Appendix 7 – Framework for Safety Management Systems (SMS) (see also Chapter 3, 3.3.4 and Chapter 8, 8.7.3.4), (http://www2.icao.int/en/ism/ICAO%20Annexes/Annex%206.pdf).*

3) *ICAO Safety Management Manual (SMM), Second Edition, 2009 – Document 9859, (http://www.icao.int/anb/safetymanagement/DOC_9859_FULL_EN.pdf).*

4) *FAA Order 8000.369, Safety Management System Guidance, Effective Date: 09-30-2008, (http://www.faa.gov/documentLibrary/media/Order/8000.369.pdf).*

5) *FAA Order VS 8000.367, Aviation Safety (AVS) Safety Management System Requirements (Appendix B: Product/Service Provider SMS Requirements)), Effective Date: 05-14-2008, (http://www.acsf.aero/attachments/wysiwyg/12/FAA_ORDER_VS8000.367_SMS_Requirements.pdf).*

Part A – An Introduction to SMS

4 Background

4.1 What is a Safety Management System (SMS)?

The FAA Aviation Safety organization (AVS) has defined an SMS as:

"…a formal, top-down, organization-wide approach to managing safety risk and assuring the effectiveness of safety risk controls. It includes systematic procedures, practices, and policies for the management of safety risk."[1]

Transport Canada's SMS definition provides further detail:

"...a businesslike approach to safety. It is a systematic, explicit and comprehensive process for managing safety risks. As with all management systems, a safety management system provides for goal setting, planning, and measuring performance. A safety management system is woven into the fabric of an organization. It becomes part of the culture, the way people do their jobs."[2]

4.2 SMS Requirements: ICAO and FAA

The ICAO has revamped its standards and recommended practices to reflect a systems approach to safety management. This coincides with the FAA's move toward a systems approach for oversight over the past several years. Because of the global nature of the aviation system and the diverse relationships between organizations, SMS functions need to be standardized to the point that they have commonly recognized meaning, both domestically and internationally.

In 2009, the ICAO Council agreed that the issue of an *SMS Framework* suitable for organizations responsible for type Design or Manufacture of aircraft should be re-examined in the future, particularly the application of a standard framework, in broad consultation with both States and industry. It decided that an applicability date of November 14, 2013 for the SMS provisions would allow sufficient time for States to establish corresponding regulations and for industry to implement them.[3] ICAO specified that when States apply SMS standards to a D&M company within their country, it should contain as a minimum:

1) Identify safety hazards;
2) Ensure the implementation of remedial action necessary to maintain agreed safety performance;
3) Provide for continuous monitoring and regular assessment of safety performance;
4) Aim at a continuous improvement of the SMS overall performance;
5) Clearly define lines of safety accountability throughout the organization, including a direct accountability for safety on the part of senior management.

[1] **Federal Register** Volume 75, No. 214, page 68242; Friday, November 5, 2010

[2] http://www.tc.gc.ca/publications/BIL/TP13739/PDF%5CHR/TP13739b.pdf

[3] http://www.paris.icao.int/news/200906_amendments_to_annexes_annex8.htm

The ICAO *SMS Framework* (cited in the ICAO Annex 6) consists of four components and twelve elements, and its implementation shall be commensurate with the size of the organization and the complexity of the services provided.

1) Safety Policy and Objectives,
2) Safety Risk Management (SRM),
3) Safety Assurance (SA), and
4) Safety Promotion.

The D&M *SMS Framework* components align with the ICAO Annex 6 *SMS Framework* components. While Annex 6 pertains to operators, the FAA anticipates Annex 8, pertaining to design and manufacturers will use the same components in defining its SMS. Additionally, the D&M *SMS Framework* provides more details and proposes new concepts to facilitate a D&M organization's SMS implementation.

4.3 The Process Used to Develop the D&M SMS

In October 2009, the Aircraft Certification Service (AIR) chartered a team to develop SMS for D&M organizations. The team is comprised of representatives from Aircraft Certification and Manufacturing Inspection offices, including management personnel. The team also includes contractors experienced in aviation, engineering, manufacturing, and SMS.

The team is identified as the Manufacturers Safety Management System (MSMS) Team. The term Manufacturer (in MSMS) was chosen to align with the ICAO definition, which combines manufacturing and engineering under "Manufacturer."

The team conducted a review of existing SMS documents/papers/literature from academia, industry, foreign regulatory agencies, and ICAO. Entities that have already implemented SMS were researched, including Flight Standards, Air Traffic, Airports, and Transport Canada.

A review of the Aviation Rulemaking Committee (ARC) report was also conducted. Input was received from FAA members supporting the ARC D&M Working Group who are contributors/members of the MSMS team.

The team created the D&M SMS guidance and tools to align with ICAO SMS recommendations and Flight Standards *SMS Framework*.

Along with the guidance and tools in this Guide, the team has also developed tools to gather information and data. The information and data collected isn't participant specific, but will be generic in nature. The team will use it to validate the Framework, Guidance material, and Oversight and Assessment tools/methodologies, and also provide the rulemaking committee data/recommendations on scalability and applicability.

4.4 An Introduction to the D&M SMS Framework

The FAA Aircraft Certification Service (AIR) has produced an *SMS Framework* for use during the pilot project as a standard set of concepts reflecting its SMS functional expectations to aid a D&M organization in voluntarily developing and implementing an SMS. The overall structure has a Developmental Guidance document that provides explanations and examples regarding its use. **The D&M *SMS Framework* is not mandatory and does not constitute a regulation.** The development and implementation of an SMS is currently voluntary and not a substitute for compliance with federal regulations or any other certificate/approval requirements.

Since the Framework is written as a functional expectations document, each of the processes detailed in the Framework is the minimum necessary for an acceptable SMS. By design, the D&M *SMS Framework* is scalable and allows organizations to integrate safety management practices into their own unique business models. Organizations are not expected to configure their systems in the exact format of the Framework or to duplicate existing programs that accomplish the same function, but to integrate it into or adapt it for the organization's policies, documents, and activities. The Framework attempts to strike a balance between flexibility of implementation and standardization of essential safety management processes.

4.5 An Incremental Approach to SMS Implementation

To make the development and implementation of the SMS more manageable, an incremental approach is adopted.

Figure 1 - SMS Implementation Levels illustrates the levels of SMS development and implementation adopted for use in the AIR D&M SMS.

This approach enables an organization to establish the basic building blocks (Levels 1 and 2) of safety management before implementing the more complex activities of integrating SRM and SA Levels 3 and 4 – see Section 8 Additional Information on SRM and SA Integration.

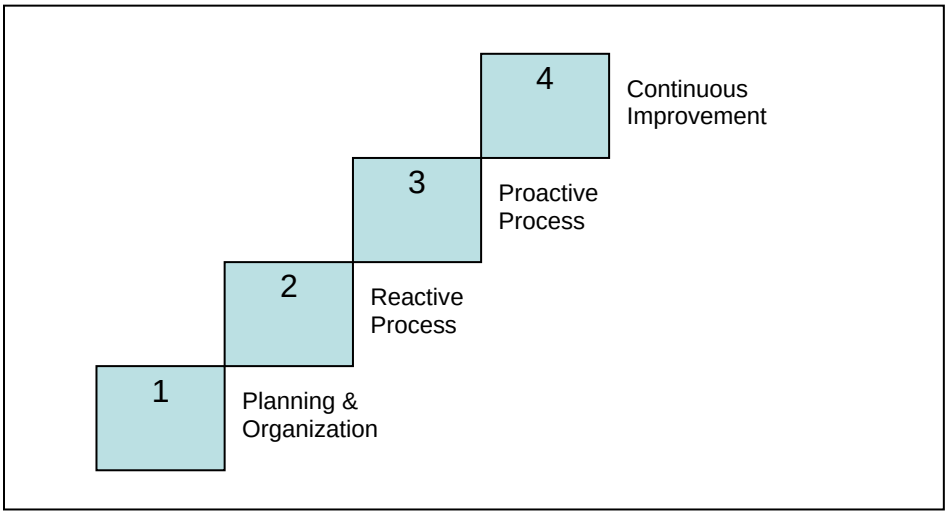


Figure 1 - SMS Implementation Levels

4.5.1 Level One – Planning and Organization

This is the starting point of the implementation process; it is a time for the organization to gather information, evaluate corporate goals and objectives, and determine the viability of committing resources to an SMS implementation effort.

The formal start of this level is the FAA/Participant Orientation Briefing and Kickoff meeting, which includes performing the preliminary gap analysis.

This level is completed when level one outputs are accomplished and upon successful completion of an exit level meeting.

4.5.2 Level Two – Reactive Process – Basic Risk Management

The objectives of Level Two are to:

1) Correct known deficiencies in safety management practices and operational processes; and
2) Plan, organize, and prepare the organization for further SMS development. This will include complying with the expectations in APPENDIX A: D&M *SMS Framework*.

At this level, the organization develops and implements a basic SRM process. At this phase, the organization develops an understanding of hazards and responds with appropriate systematic application of preventative or corrective actions. This allows the organization to react to unwanted events and problems as they occur and develop appropriate remedial action. For this reason, this level is termed 'reactive.' While this is not the final objective of an SMS, it is an important step in the evolution of safety management capabilities.

4.5.3 Level Three – Proactive Processes, Looking Ahead

The D&M *SMS Framework* expects SRM to be applied to the initial design of systems, processes, organizations, and products, development of D&M procedures, and planned changes to D&M processes. The activities involved in the SRM process require the careful analysis of systems and tasks involved; identification of potential hazards in these functions, and development of risk controls. The risk management process developed at Level Two is used to analyze, document, and track these activities. Because the organization is now using the processes to look ahead, this level is termed 'proactive.' At this level, however, these proactive processes have been implemented but their performance has not yet been proven.

4.5.4 Level Four – Continuous Improvement

The final level of SMS maturity is the continuous improvement level. Processes have been in place and their performance and effectiveness have been verified. The complete SA process, including continuous monitoring and the remaining features of the other SRM and SA processes are functioning. A major objective of a successful SMS is to attain and maintain this continuous improvement status for the life of the organization.

4.6 D&M SMS Framework

AIR's D&M *SMS Framework* is supplemented by a Developmental Guidance document, a Definitions and Acronyms document (see Section 14), and a Gap Analysis Tool (Excel Workbook). The Developmental Guidance provides explanations and examples in a separate document, which replicates each Framework section, followed by the related developmental

guidance. The Definitions and Acronyms document (see Section 14) has been developed to clarify terms and acronyms used within the Framework for the purposes of the D&M SMS Pilot Project. The Gap Analysis Tool is designed to assist an organization in analyzing its existing programs, systems, and activities with respect to the Framework; in identifying areas not being performed (gaps); and in tracking its SMS implementation progress.

For clarity, AIR has organized the Framework's *functional expectations* using a hierarchical structure of *components*, which are composed of *elements*, to focus the organization's application of the Framework in developing and implementing an SMS. The Framework was created to emphasize "what to do" rather than "how to do it." Since the Framework objectives and functional expectations are the minimum necessary for a functional and comprehensive SMS under the pilot project, they are presented in a requirements-oriented tone. Since the Framework needs to be applicable to a wide variety of organization types and sizes, by design it is scalable and allows organizations to integrate safety management practices into their unique business models.

A key success factor in an SMS is the fostering of a *safety culture* that enables an organization's people to function together in a manner that promotes safety awareness throughout.

"An organization's culture consists of its values, beliefs, legends, rituals, mission goals, performance measures, and sense of responsibility to its employees, customers, and the community."[4]

The safety culture consists of psychological (how people think and feel), behavioral (how people and groups act and perform), and organizational or systematic (the programs, procedures, and organization of the enterprise) elements. For this reason, this Framework includes expectations for policies that will provide objectives for organizational functions. These functions include an effective employee safety reporting system and clear lines of communication both up and down the organizational chain regarding safety matters.

Since many organizations must interact with more than one regulator and other parts of the FAA, AIR has tried to minimize the need for different management systems, by leveraging content from the following:

1) Notice of Proposed Rule Making (NPRM) Part 5: Safety Management Systems
2) FAA Order VS 8000.367, Appendix B
3) FAA Flight Standards Service (AFS) *SMS Framework* (for operators and maintenance organizations)
4) ICAO *SMS Framework* located in Annex 6: Operation of Aircraft.

4.7 D&M SMS Pilot Project Objectives

The MSMS pilot project team has identified five high-level objectives for conducting the D&M SMS pilot project:

1) Provide feedback to AIR rulemaking activities needed to implement SMS;
2) Develop and validate the draft D&M SMS Framework;

[4] Manuele, Fred A., On the Practice of Safety, John Wiley & Sons, 2003, Hoboken, NJ.

3) Develop and validate the draft guidance material;
4) Collect information that will assist in the determination of applicability and scalability (which companies will be required to implement) of a SMS rule for D&M organizations; and
5) Develop draft D&M SMS assessment and oversight processes and tools.

5 Roles, Responsibilities, and Relationships

Participation in SMS development is completely voluntary and may be terminated at any time by the organization or the FAA. Pilot Project participants will benefit by being early adopters of an SMS should implementation be mandated through future U.S. Federal Aviation Regulations. In addition SMS is an ICAO Annex 6 requirement and as such there may be a need for organizations that sell products outside of the U.S. to have an SMS consist with the ICAO SMS requirements. Because the pilot project is voluntary a participant may implement any SMS process and procedure at any time. Neither FAA oversight organizations (MIDO, CMO, ACO) or the PMT are currently authorized to approve or accept SMS programs since no regulatory standard exists on which to base those actions.

Figure 2: Organizational Chart for MSMS Team outlines the organization of the team for the execution phase of this pilot project.

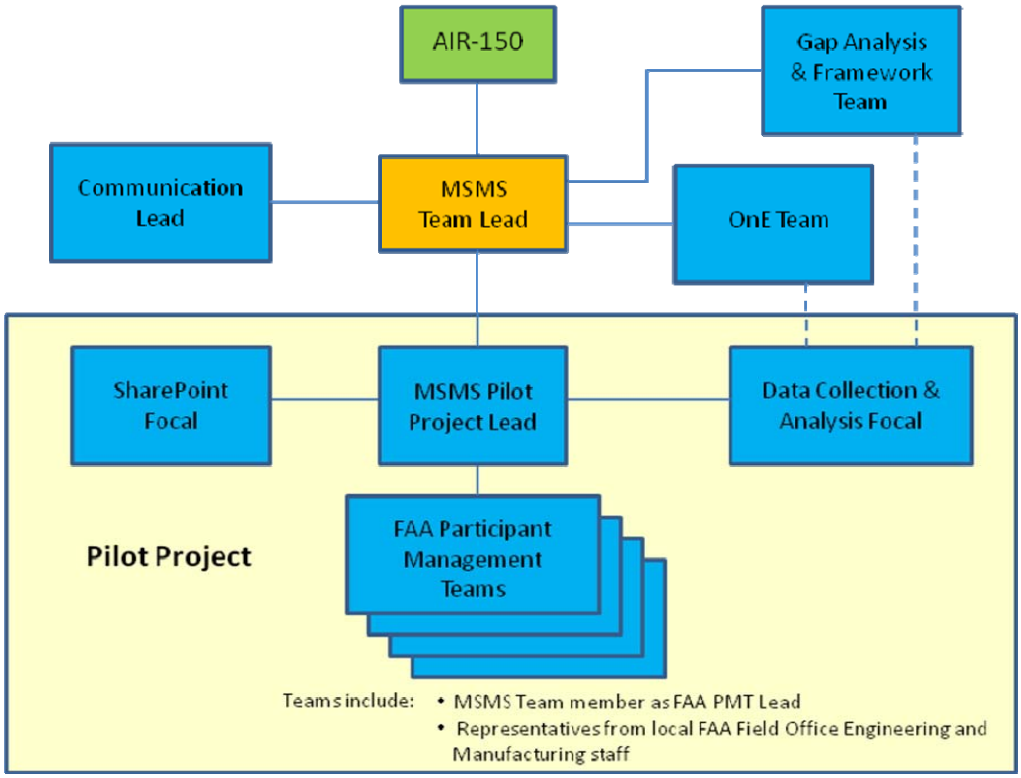


Figure 2: Organizational Chart for MSMS Team

5.1 AVS Office of Safety Management Design & Analysis – AIR-150

The program office responsible for leading the development and implementation of SMS with the Aviation Certification Service (AIR) is the Safety Management Design and Analysis Branch – AIR-150. This office provides policy and guidance on externally oriented SMS requirements and interfaces, provides support to the AIR Director and Executive Steering Committee in execution of the AIR SMS doctrine, provides direction, guidance, and coordination with headquarters and field divisions in the development of SMS policies and procedures.

5.2 MSMS Team

The MSMS team is drawn from personnel from across the AIR directorate, the U.S. Department of Transportation (DOT), and consultant organizations to:

1) Develop and maintain a prototype *SMS Framework*, guidance, and training requirements for D&M organizations;
2) Develop and maintain SMS data collection and analysis tools;
3) Standardize concepts, functional requirements, and terminology across AIR for activities managed and sponsored under the D&M SMS initiative;
4) Provide oversight and assess SMS pilot projects;
5) Develop and use standardized orientation and guidance materials for SMS; and
6) Coordinate and manage AIR SMS Participant Management Teams (PMTs) to assist field offices and participant organizations in development and implementation of this voluntary SMS pilot project.

5.2.1 MSMS Team Lead

The MSMS Team Lead is responsible for providing a focused vision, leadership, and direction to the MSMS team in the execution of the projects overall objectives.

5.2.2 MSMS Pilot Project Lead (PPL)

The Pilot Project Lead (PPL) is responsible for leading and coordinating the FAA Participant Management Teams (PMTs) execution of the pilot project.

This individual is responsible for:

1) Coordinating and managing the AIR PMT;
2) Maintaining the MSMS Pilot Project Tracking Matrix and schedule;
3) Updating the MSMS Integrated Pilot Project Planning (IP3) document;
4) Providing feedback to PMTs about decisions made at the MSMS leadership level;
5) Determining when PMTL responsibilities can be transitioned to FAA Field Office personnel;
6) Providing final acceptance for progression to the next step/level of SMS maturity. (Progression recommendations come from AIR PMT members and AIR PMTL);
7) Developing standardized outreach information for AIR SMS activities;
8) Serving as the Data Collection and Analysis focal, and in that role:
    a) Developing a list of specific data to be collected during the pilot project. This includes time spent to accomplish specific goals/tasks, costs involved, travel, time spent on site with participant, etc.
    b) Developing a database and process to input, store, access, and catalog received data.
    c) Developing a process for analyzing the data and creating output methods (charts/narrative) for users to review the data;
9) Providing status/updates to senior AIR Management Team throughout the pilot project period of performance; and
10) Producing a lessons learned report.

5.2.3 FAA Participant Management Team (PMT)

Each PMT consists of the following FAA personnel:

1) Two people from the MSMS team: a lead and a support member;
2) One to two Aviation Safety Inspector(s) (ASI) from the geographical Manufacturing Inspection District Office (MIDO), Certificate Management Office (CMO), and/or Manufacturing Inspection Satellite Office (MISO); and
3) One to three Aviation Safety Engineer(s) (ASE) from the geographical Aircraft Certification Office (ACO).

The PMT is responsible for participating in the orientation and assessment meetings. The PMT will review the participant's gap analysis, implementation plan, SMS procedures and processes, and assess the participant's accomplishment at each level of the SMS implementation.

5.2.4 AIR Participant Management Team Lead (PMTL)

The PMTL has been selected from the MSMS Team to coordinate all formal interaction with the participant. This will include: meetings, telecons, and reviews for step/level progression, etc.

The PMTL will also:

1) Provide direction and guidance to the PMT;
2) Develop a communication process with the participant; determine how communication will take place (telephone, email, letters, etc.);
3) Maintain a schedule for target/goals, i.e., exit level meeting dates;
4) Provide assistance, as requested, to the participant;
5) Participate in frequent (suggested to be weekly or bi-weekly) meetings with the participant;
6) Review the participant's implementation plan and other documents and provide objective input;
7) Discuss the requirements of exit criteria for all maturity phases of SMS implementation with the participant;
8) Receive pilot project inputs from both the participant and assessment or PMT, including ACO, MIDO, CMO, etc.;
9) Collect data required for Pilot Project Data Analysis, document lessons learned;
10) Coordinate with MSMS PPL for information, guidance, direction, and executive visits; and
11) Provide status/updates to the PPL throughout the Pilot Project.

5.2.5 FAA Field Office Personnel

The FAA Field Office Personnel include, but are not limited to: ASI, ASE, Flight Test pilot, or engineer. Office managers will provide the PPL the names of proposed PMT members. The MSMS leadership team must agree to the names before the names are added to the MSMS Pilot Project Tracking Matrix. The PPL/MSMS Team Lead will solicit names from office managers.

Personnel assigned to the PMT will receive direction and guidance from the PMTL.

Initially field office personnel will provide comments only on participant produced processes, procedures, etc. They will have no authority to accept outputs from participants as this task is for the MSMS PMTL. Field personnel will review processes and procedures prior to forwarding (with comments) to the PMTL. The PMTL will review and forward to the PPL (with comments/recommendation). As field personnel experience and confidence increases, the PPL may grant them more authority.

Field office personnel assigned to the PMT are responsible for the following:

1) Complete all SMS training requirements;
2) Provide status/updates to their office management throughout the pilot project;
3) Provide assistance, as requested by the PMTL throughout the pilot project;
4) Participate in PMT meetings/telecons;
5) Participate in participant meetings/telecons and site visits;
6) Assist in reviewing the participant's implementation plan and other documents and provide objective input; and
7) When requested by the PMTL, assess the SMS procedures and processes and provide comments to the PMTL.

5.2.6 Certificate Management (CM)

The AIR D&M SMS pilot project is not expected to interfere with an ASI's Certificate Management (CM) responsibilities with respect to their assignment to a Production Approval Holder (PAH). Any changes or additions to a PAH's FAA approved quality system will continue to be processed and approved in accordance with FAA Order 8120.2 and local office policies. However, the PMT will review any SMS procedures and processes that are also under the FAA approved quality system, in accordance with this plan and the D&M SMS Pilot Project Guide. Any changes or recommendations to the companies' Policies and Procedures (P&P) must be equally agreed to between the PMT and Principal Inspector (PI).

MIDO and ACO personnel will continue to manage PI audits / Aircraft Certification Systems Evaluation Program (ACSEP)/Type Certificate (TC)/Supplemental Type Certification (STC), per existing procedures.

Technical discussions between team members and the participant may occur with PMTL concurrence.

5.2.7 SharePoint Focal

A SharePoint website will be used to share data, communication, and information between the participant and the PMT. The SharePoint Focal assists with the development of the SharePoint site and will manage and maintain the system to ensure validity, security, currency, and accessibility to its users. User accessibility and security to the SharePoint website will be controlled to protect each participant's data and information. Only the participant, the MSMS team, and the PMT will have access to participant's data.

The PMT assessment of SMS policies, procedures, and data will be done using SharePoint. Each participant will upload their policies, procedures, and data to their own tab on SharePoint. The PMT will review the participant's policies, procedures, and data and then provide FAA acceptance and or comments on SharePoint. Participants' data will be purged when no longer needed for the FAA assessment.

The SharePoint website will also include:

1) Frequently Asked Questions (FAQs) (non-propriety);
2) Generic Lessons Learned information (Propriety data will not be shared);
3) FAA SMS guidance documents;
4) Gap analysis and assessment tools; and
5) Other SMS information.

5.2.8 Data Collection and Analysis Focal

During the pilot project data, lessons learned and other information will be collected to assist in the development of the D&M *SMS Framework*, policy, and processes. It is anticipated that the data and information will be general and not technical in nature. If propriety data is received it will not be preserved or shared outside the MSMS team.

The Data Collection and Analysis Focal is responsible for:

1) Developing a list of specific data and information to be collected during the pilot project;
2) Developing and maintaining a database and process to collect, store, access data, information, lessons learned, surveys, and feedback, etc.;
3) Developing a process for analyzing data and lessons learned and create output methods (charts, narrative, reports) for the MSMS team;
4) Collecting lessons learned data and feedback on process improvements to the SMS and pilot project processes. (A Lessons Learned and feedback form will be provided to the participants during each major event or visit by the PMTL.);
5) Coordinating lessons learned data with the Lessons Learned Review Board.

5.3 Communication between the PMT and Participant Organizations

The purpose of the formal communication process is to maintain a consistent AIR MSMS Team message. Formal communications/decisions between the participant and the PMT will be through the PMTL and the participant SMS Point of Contact (POC). Formal decisions will be in writing (email) for standardization and retention purposes. Formal communications are deviations, clarifications (interpretation), and improvements concerning the gap analysis/tool, D&M *SMS Framework*, and FAA guidance material. These formal communications will be coordinated though the PMTL and the PPL to maintain standardization. The PPL will consult with the MSMS leadership team for an official response.

The MSMS Leadership team provides policy and guidance on internally and externally oriented SMS requirements and interfaces.

5.4 Participant Organization SMS POC

This individual represents the participant organization as SMS Project Manager (or similar) and acts as the SMS POC for their SMS activities. This POC will be the primary contact for the FAA and the FAA PMTL.

During the initial implementation of SMS, the POC will coordinate with the FAA PMT to develop a useable and realistic communication process for the FAA PMT. The Participant POC is expected to manage and report on the status and momentum of the participant organization's execution of the SMS Implementation Plan. Difficulties, roadblocks, or delays must be reported to the FAA PMT so that alternative solutions can be implemented.

Part B – Implementing SMS in D&M Organizations

6 Introduction to the Implementation Processes

This part provides a copy of the D&M *SMS Framework* and an overview of the tools necessary for an organization to implement an SMS. It also contains processes the FAA will utilize to perform oversight and evaluation activities.

Specifically, the Guide provides expectations, procedures, and guidance necessary to implement an SMS. These are:

1) An introduction to the D&M *SMS Framework* (Section 8);
2) Pilot project process for implementation level 1 (Section 9);
3) Pilot project process for implementation level 2 & 3 (Section 10);
4) FAA assessment and oversight requirements of the SMS assessment (Section 11); and
5) Additional information on SRM & SA integration (Section 12).

The Guide also includes the following appendices:

1) The D&M *SMS Framework* document – APPENDIX A: D&M *SMS Framework*;
2) A description of the implementation levels – APPENDIX B: D&M SMS Pilot Project Levels;
3) Screenshots illustrating the content and format of the Gap Analysis Tool (GAT) – APPENDIX C: Tools and Templates; and
4) A brief overview of the System Description and Hazard Identification process – APPENDIX D: System Description & Hazard Identification Process.

This guide will assist FAA PMTs in evaluating an organization's SMS program and participating in further development of implementation and oversight strategies.

6.1 D&M SMS Framework

The MSMS Team has developed a D&M *SMS Framework* document; it is the current 'standard' for voluntary implementation of SMS by D&M organizations. It was initially based in scope and format on the AFS *SMS Framework* developed for organizations operating under 14 CFR Part 121 regulations.

The original issue of the D&M *SMS Framework* (Revision A) was developed with the current requirements provided in Annex 6 of the conventions of the ICAO, and the current requirements of FAA Order VS 8000.367, Appendix B, in mind, and it was closely aligned with the current ICAO *SMS Framework*.

The current version of the D&M *SMS Framework*, (Revision B) was issued so that it more closely aligns with the Notice for Proposed Rulemaking (NPRM) Part 5 and to eliminate areas of duplication. For the purposes of the pilot project, the D&M *SMS Framework* provides a slightly deeper level of detail; however, the overall intent and focus are better aligned. The revised D&M *SMS Framework* remains aligned with the ICAO *SMS Framework*. In addition, some of the more detailed content that was removed from the Framework may be found in the Developmental Guidance.

6.2 Developmental Guidance Material

The Developmental Guidance (DG) document provides assistance to an organization in developing their SMS using the D&M *SMS Framework*. The DG contains further explanation and where appropriate provides examples on how to meet the framework requirements.

Note: *The DG is provided as a separate document.*

The D&M SMS DG document replicates the structure of the D&M *SMS Framework*'s *functional expectations* using a hierarchical structure of *components*, which are composed of *elements* and their subordinate *sub-elements*. The D&M *SMS Framework* structure employs the four basic components of a safety management system: Safety Policy and Objectives, SRM, SA, and Safety Promotion.

6.3 Gap Analysis Process and Assessment Process Tools

The Gap Analysis Tool (GAT) is provided as a separate Microsoft Excel spreadsheet, with embedded instructions on its use on the first tab of the workbook.

The Preliminary GAT assists the organization in conducting an initial, high-level assessment on existing organizational programs, systems, and activities with respect to the Components, Elements, and Sub-Elements found in the functional Expectations of the SMS Framework. This initial assessment provides an initial look into how compliance is assessed with the SMS.

Two types of gap analysis processes are performed, see paragraphs 6.3.1and 6.3.3.

6.3.1 Preliminary Gap Analysis

The Preliminary Gap Analysis (PGA) process is performed onsite with the assistance of the FAA PMT. The participant POC and the company organizational leaders contribute as subject matter experts in the PGA discussion. The PGA represents an "executive overview," which is a high-level subjective analysis of where the organization stands with respect to the D&M *SMS Framework*. An initial step in developing an SMS is for the organization to analyze and assess its existing programs, systems, processes, and activities with respect to the SMS functional expectations found in the D&M *SMS Framework*. This process is called a "gap analysis," the "gaps" being those elements in the D&M *SMS Framework* that the organization is not already performing.

The objectives of the PGA are to:

1. Ensure the organization and FAA have a common understanding of the Gap Analysis Process;
2. Help the organization describe itself using a set of SMS system segments;
3. Develop a common understanding of the D&M *SMS Framework* Expectations in the context of the organization and its operations;
4. Obtain an initial understanding of the organization's processes across system segments to determine whether the processes meet the D&M *SMS Framework* Expectations.

6.3.2 Methods of System Segment Determination

One of the first steps in performing the PGA is to determine how to identify the organization's "segments." These segments are used as column headers for the PGA and compartmentalize the organization allowing in-depth analysis. The organization performing the PGA makes a decision

as to whether the expectation(s) contained in each element of the Framework is achieved within that particular segment. For the PGA, this decision is made fairly quickly and from a high level. For the Detailed Gap Analysis (DGA), this decision is made after a thorough and complete analysis of the segment from the product, process, and organizational perspectives. See Appendix D: System Description and Hazard Identification Process for more information.

The simplest and most obvious ways to determine what system segments to use are:

(1) Using segments that are organizationally, geographically, or departmentally related (i.e., engineering, manufacturing, marketing, etc.);

(2) Using segments that are functionally related (i.e., design, manufacturing, assembly, quality inspection, marketing, finance, etc.); and,

(3) Using segments that are product line oriented (i.e., aircraft/engine model, subassemblies, components, parts, electronic product lines, machined product lines, etc.).

However, the participant may always choose an approach of their own. Whatever approach is chosen, the participant defines the scope of its SMS through the choice of its system segments. This scope forms the basis for all hazard analysis of the organization when implementing the SRM component. It is possible that the participant may find it beneficial to adjust the scope of its SMS for the DGA as the organization learns more about what is appropriate for its business.

6.3.3 Detailed Gap Analysis

The second type of gap analysis is a more in-depth "Detailed Gap Analysis" process and is performed by the organization (with assistance of the PMT). It is a comprehensive and thorough assessment of each program, process, and control of the organization as compared to the objectives and expectations of the D&M *SMS Framework*. Depending upon the size and complexity of the organization, the DGA may take 4 to 6 months to complete. The DGA is a "living" process and will be continually updated as SMS implementation progresses. Both the Preliminary and Detailed Gap Analysis processes cover all areas of company operations and all elements of the D&M *SMS Framework*.

6.3.4 Implementation Plan

Based on the results of the DGA process, an implementation plan is prepared to "fill the gaps", the 'gaps' being those elements in the D&M *SMS Framework* that have not completely met the organization's expectations (e.g., are <u>not</u> already being performed). The SMS implementation plan is a realistic approach for the implementation of an SMS that will meet the organization's safety objectives. It describes in detail how and when the organization will achieve its corporate safety objectives and how it will meet any new or revised safety requirements, regulatory or otherwise. At each level (1 through 4), top management's approval of the implementation plan must include allocation of necessary staffing and resources. The implementation plan also describes who is responsible to track and validate implementation of each new or revised procedure/process. The implementation plan focuses on the SMS within the scope of the participant's system description.

The GAT includes a worksheet (pre-populated with the gaps identified from the DGA) to aid in creating the implementation plan. In addition to the implementation plan within the DGA a written narrative should be used to describe the details of the implementation. The implementation plan need not be complex or excessively detailed, but should provide a basic

roadmap to meet the overall objective stated in the ***SMS Framework.*** The implementation plan should also span the entire SMS development process through all levels of maturity and should be updated as necessary (along with the detailed gap analysis) as the projects progress. The organization's SMS planning group should meet regularly with top management to assess progress of the implementation plan, and receive resources commensurate with the task at hand.

Examples of what could go into the narrative are: Who is responsible for the execution of the SMS plan; What procedures / processes will be created or revised; How will the company determine if the procedure/process meets the performance expectations and if not what actions are necesary; Allocation of necessary resources; Expected completion date; A brief description of the manual/procedures affected (*Some companies have created a high level SMS manual that incorporates the general SMS requirements that affects each organization and within the SMS manual they have a matrix or index pointing to the procedures or processes that support the SMS).*

6.3.5 Assessment Process Tools

The purpose of these tools is to convey the expectations of the D&M *SMS Framework* in a user-friendly spreadsheet format. Additional room for the inclusion of source document references and progress/status by company divisions is also provided. The titles of system segments (the breakdown of the company participating in the pilot project) at the top of the gap analysis tools may be customized to fit the individual structure of the organization. Additional sheets enable the development of an Implementation Plan for the attainment of each SMS implementation level, and a form to enable the PMT to document their assessment of each.

If conflicts between the language in the gap analysis tools and the D&M *SMS Framework* are found, the language in the D&M *SMS Framework* should prevail. The key objective of the gap analysis is to determine whether or not existing programs or processes in the company meet the expectations delineated in the D&M *SMS Framework*, so this objective should be kept in mind throughout the gap analysis and planning process.

7 Introduction to the D&M SMS Framework

The structure of the D&M *SMS Framework* employs the four components (basic building blocks) of an SMS: Safety Policy and Objectives, SRM, SA, and Safety Promotion. These four components are essential for an SMS and come directly from the SMS principles in Section 4 – Background.

The unabridged version is available in APPENDIX A: D&M *SMS Framework*.

7.1 Safety Policy and Objectives (Component 1.0)

Effective management systems must define policies, procedures, and organizational structures to accomplish their goals. The Framework's Safety Policy and Objectives Component outlines expectations in the Elements below, which in turn provide the foundation for the functional SMS Components 2.0 and 3.0 (SRM and SA).

1) Safety Policy (Element 1.1),
2) Management Commitment and Safety Accountability (Element 1.2),
3) Designation and Responsibilities of Required Safety Management Personnel (Element 1.3),

4) Emergency Preparedness and Response (Element 1.4), and
5) SMS Document and Records (Element 1.5).

7.2 Safety Risk Management (SRM) (Component 2.0)

SRM is a formal system of hazard identification and analysis and risk control (sometimes termed *mitigations*), used to assess systems at both the organizational and product levels. SRM foundation is a system definition of the organization that consists of its structures, processes, and procedures, as well as the people, equipment, and facilities used to accomplish the organization's mission. The system description should completely explain the interactions between the organization (facilities, hardware, software, people, etc.) and its environment in sufficient detail to identify hazards and perform risk analyses.

SRM Framework Elements essential in controlling risk to acceptable levels and their subordinate Sub-Elements are:

1) Hazard Identification and System Analysis (Element 2.1),
2) System Description and Analysis (Sub-Elements 2.1.1),
3) Identify Hazards (Sub-Elements 2.1.2),
4) Risk Assessment and Control (Element 2.2),
5) Analyze Safety Risk (Sub-Elements 2.2.1),
6) Assess Safety Risk (Sub-Elements 2.2.2), and
7) Control/Mitigate Safety Risk (Sub-Elements 2.2.3).

7.3 Safety Assurance (SA) (Component 3.0)

Once SRM controls are identified and employed, an organization must ensure that the SRM designed and implemented controls continue to be used as intended and continue to be effective as the environment changes. The SA function provides for this, using system safety and quality management concepts and processes. SA may also identify hazards not previously recognized. As part of the SA function, the analysis of data and system assessment functions must alert the organization to significant changes in the operating environment, possibly indicating a need for system change to maintain effective risk controls. Also, a change management course of action should identify changes within the organization that may affect established organization processes, procedures, products, and services. Prior to implementing changes, this method should describe preparations to ensure safety performance.

SA Framework Elements for assuring safety and the subordinate Sub-Elements are:

1) Safety Performance Monitoring and Measurement (Element 3.1),
2) Continuous Monitoring (Sub-Element 3.1.1),
3) Internal Audit (Sub-Element 3.1.2),
4) Internal Evaluation (Sub-Element 3.1.3),
5) Investigation (Sub-Element 3.1.4),
6) Employee Reporting and Feedback System (Sub-Element 3.1.5),
7) Analysis of Data (Sub-Element 3.1.6),
8) System Assessment (Sub-Element 3.1.7),
9) Management Review (Sub-Element 3.1.8), and
10) Management of Change (Element 3.2).

7.4 Safety Promotion (Component 4.0)

The organization's upper management must promote safety as a core value with practices that support a sound safety culture. The organization must make every effort to communicate its goals and objectives as well as the current status of the organization's activities and significant events. Additionally, the organization must also put in place processes that allow for open communication among employees and the organization's management in an environment of collaboration, trust, and respect. It is important that all employees have appropriate skills and training to identify potential safety hazards, to know how to report safety concerns, and to know that it is their responsibility to do so.

The Safety Promotion Component provides the *SMS Framework* expectations for establishing and implementing these functions through the following Elements and Sub-Elements:

1) Competencies and Training (Element 4.1),
2) Personnel Expectations (Competence) (Sub-Element 4.1.1),
3) Training (Sub-Element 4.1.2), and
4) Communications and Awareness (Element 4.2).

8 Additional Information on SRM and SA Integration

Once SRM organizational and product risk controls are developed and determined to be capable of bringing the risk to an acceptable level, they are employed operationally.

Then the SA function takes over to ensure that the risk controls are implemented and that they continue to achieve their intended objectives. The SA function also provides for assessing the need for new controls because of changes in the operational environment. However, some identified risks may not need controls, but only monitoring because of the improbability of their occurrence. The risk analysis should ascertain when monitoring is a sufficient response, when risk mitigation or control activities are the appropriate responses to an identified risk, or when a product or process change is needed.

Figure 3 below shows how the SRM and SA functions relate to one another when SRM leads to the need for risk controls.

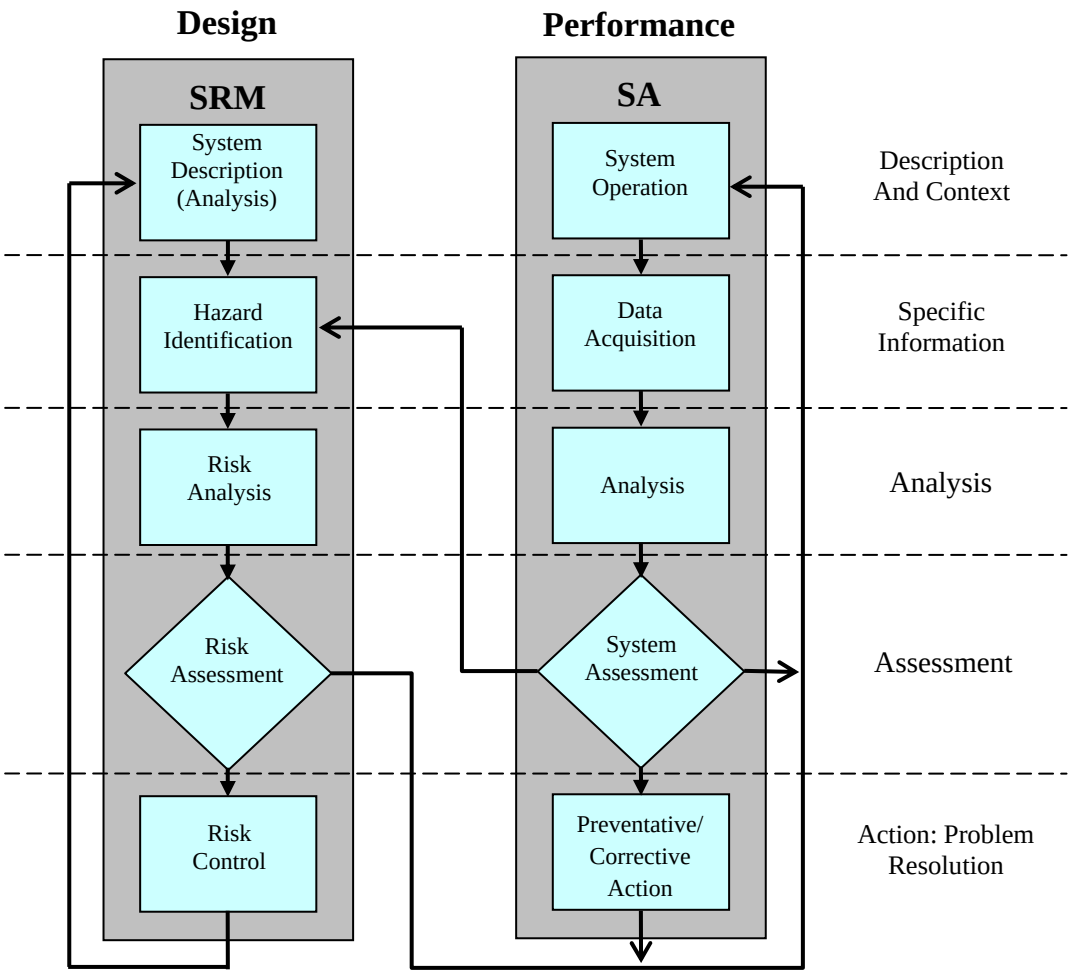


Figure 3: SRM and SA Process Relationship

9 Pilot Project Process for Implementation Level 1

The "implementation Level 1" process, planning and organization, is the implementation process starting point. It focuses on the organization and development of the implementation plan. The following activities are to be accomplished in Level 1 before proceeding to Level 2:

1) Orientation Briefing and Preliminary Gap Analysis;
2) Defined Safety policy;
3) Detailed Gap Analysis, and Implementation Plan;
4) SMS training plan for all employees participating within the scope of the system description; and
5) Successful completion of an exit Level one validation meeting.

Figure 4: Process Outline for Implementation Level 1 provides an overview of this Level 1 process.

9.1 Preparation Prior to the Orientation Briefing

The PMTL will send the D&M SMS information package (defined below) to the participant organization and PMT members to prepare them for the orientation briefing.

1) D&M SMS Information Package:
    a) Orientation Briefing materials,
    b) D&M SMS Pilot Project Guide – the 'Guide',
    c) DG document,
    d) GAT, and
    e) System Description Hazard ID process.

The PMTL will hold a pre-orientation briefing telecon with the participant and PMT members to discuss the following key items:

1) Orientation meeting agenda, expectations, and outcomes;
2) Senior-level participation and commitment to the implementation of SMS by actively supporting and providing staffing and resources to achieve pilot project goals;
3) FAA expectation that the company's executive level management attend the four- hour SMS briefing on the first day;
4) Need for the company's departmental/organizational subject matter experts to participate in the two-day PGA meeting;
5) The role of company POC and the personnel needed to attend the briefing and the PGA;
6) Need for the participant to review the orientation briefing (PowerPoint™ slides) prior to the orientation meeting;
7) Purpose of the Guide;
8) Need for the participant to identify the scope of the organization taking part in the pilot project. This will include a discussion of the system description task prior to starting the PGA;
9) Use of the PGA tool; and
10) Meeting logistics e.g. meeting room location, security, etc.

A more detailed checklist is available for the PMTL to use.

9.2 Orientation Briefing

The orientation briefing will constitute the launch or kick-off of the participant's involvement in the D&M SMS pilot project. The PMTL will conduct the following briefings:

1) Orientation briefing to local FAA Field Office personnel assigned to the PMT, and
2) Orientation briefing to the participant organization.

9.3 Checklist and Required Documents

An Exit Level Checklist will be completed by PMTL performing the organization's assessment and provided to the organization. In addition, the assessment team should obtain copies of specific documentation to accompany the checklist for each level as shown below:

1) Exit Level 1 Checklist (See Appendix B - Implementation Level 1: Planning and Organization) with all items completed (initialed) plus:

    a) Safety Policy,
    b) Completion of DGA,
    c) Comprehensive SMS Implementation Plan for the entire* organization through SMS Implementation Level 4 (See appendix 4);
    d) SMS Training Plan for all employees; and
    e) Completion of an exit Level 1 validation meeting.

**Entire organization participating within the scope of the system description*

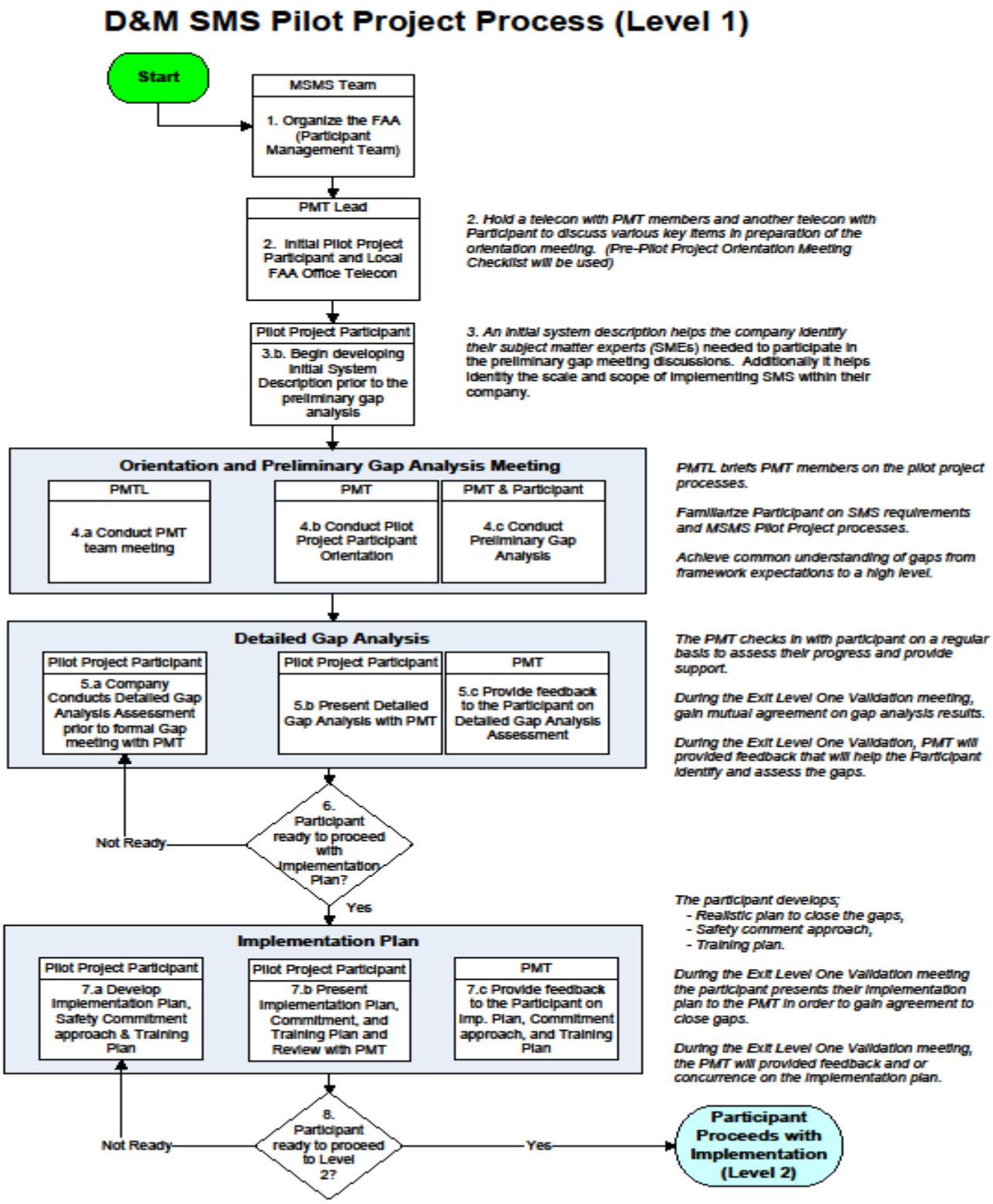


Figure 4: Process Outline for Implementation Level 1

10 Pilot Project Process for Implementation Levels 2 & 3

The two SMS implementation levels that will be subject to assessment are Levels 2 & 3. Organizations may develop their own SMSs in a modular fashion across departments or across the functions of their respective organizations. However, attainment of the implementation levels described below is based on the existence of a system encompassing all of applicable items listed in GAT. An SMS Pilot Project objective is to work with an organization to encourage its development of a comprehensive SMS covering the entire* organization.

**Entire organization participating within the scope of the system description*

10.1 Implementation Level 2: Reactive Process, Basic Risk Management

At Level 2, the organization develops and implements a basic SRM process. The organization will plan, organize, and prepare the organization for further SMS development. Information acquisition, processing, and analysis functions are implemented and a tracking system for risk controls and corrective actions are established.

In this phase, the organization corrects known deficiencies in safety management practices and operational processes and develops an awareness of hazards and responds with appropriate systematic application of preventative or corrective actions. This allows the organization to react to unwanted events and problems as they occur and develop appropriate remedial action.

For this reason, this level is termed 'reactive.' This will include complying with the expectations in Appendix B.

The completed assessment of this level demonstrates that the organization has successfully implemented the processes corresponding to Level 2 of this guide. At this level, all of the processes of the SMS have been designed and implemented in accordance with the GAT; however, they are only working in a reactive capacity. Sufficient data has not yet been accumulated at this point to enable proactive analysis.

10.2 Implementation Level 3: Proactive Processes, Looking Ahead – A Fully-Functioning SMS

Component 2.0 Element 2.1 (1) of the D&M *SMS Framework* expects SRM to be applied to the initial design of systems, processes, organizations, and products, development of operational procedures, new or recurring hazards identified, and planned changes to operational processes. The activities involved in the SRM process involve careful analysis of systems and tasks involved; identification of potential hazards in these functions, and development of risk controls. The risk management process developed at Level 2 is used to analyze, document, and track these activities. Because the organization is now using the processes to look ahead, this level is termed 'proactive.' At this level, however, these proactive processes have been implemented but their performance has not yet been proven.

This level will be validated when an organization demonstrates that they have successfully implemented the processes corresponding with Level 3 of this guide, Appendix B – Implementation Level 3 – , and that the performance of these processes has been demonstrated in a performance review conducted by the PMT, assisted as necessary by members of the PMT. At this level, the organization is considered to have a fully instituted SMS, however due to their relative newness the

performance and effectiveness of the SMS processes have not yet been validated for continued system effectiveness.

10.3 Checklist and Required Documents

An Exit Level Expectation Checklist will be completed by the PMTL performing the organization's assessment and provided to the organization. In addition, the assessment team should obtain copies of specific documentation to accompany the checklist for each level as shown below:

1) Exit Level 2 Checklist (See Appendix B – Implementation Level 2: Reactive Process, Basic Risk Management with all expectations completed (initialed)) plus:

    a) Data showing that SRM processes and procedures have been applied to at least one existing hazard and that the mitigation process has been initiated;

    b) Updated comprehensive SMS implementation plan for all elements to take the organization through Level 4; and

    c) Updated SMS Training Plan for all employees.

2) Exit Level 3 Checklist (Appendix B – Implementation Level 3 –) with all expectations completed (initialed) plus:

    a) Data showing that SRM processes and procedures have been applied to all Element 2.1 (1) items;

    b) Data showing that all applicable SMS processes and procedures have been applied to at least one existing hazard and that the mitigation process has been initiated;

    c) Updated comprehensive SMS implementation plan for all elements; and

    d) Updated SMS Training Plan for all employees.

Part C – Assessment of D&M Organizations

11 Overview of FAA's D&M SMS Assessment Approaches

The purpose of this section is to describe the D&M Pilot Project SMS Assessment Process. Prior to entering into the assessment process, the FAA will provide briefing materials to the pilot project participant during an orientation meeting explaining the objectives of the pilot project, SMS principles, D&M *SMS Framework*, GAT, and pilot project assessment process details.

Since the D&M SMS Pilot Project engages industry in a voluntary effort, the FAA expects to work cooperatively with organizations to evolve and refine the assessment criteria and processes. The PMT will be the key group interacting with organization's senior management, while the PMT will assess the documentation and conduct onsite implementation assessments.

11.1 SMS Participant Assessment Process

The Pilot Project assessment allows organizations to develop an SMS in a standardized approach and allows validation and acknowledgement at each level of development. The FAA recognizes that implementation of a complete SMS may be a lengthy process and may not be completed by the end of the pilot project. The FAA's assessment will cover the scope of the participant's pilot project.

The SMS assessment can be performed in an incremental manner throughout the development of the organization's SMS or as a final event prior to their advancing to another level. The organization must have met all the requirements for exiting Level 1, (see section 9-3 for Level 1 exit requirements) prior to beginning the assessment process.

Figure 5: Assessment Process Overview and the following paragraphs provide an overview of the pilot project assessment process.

11.1.1 Assessment Process Initiation

The organization's request for a SMS assessment initiates the assessment process. The request will be submitted to the PMT personnel as identified during the initial orientation meeting or as otherwise established with the organization's PMT representative. The PMTL will coordinate the scope of the assessment along with an assessment date.

11.1.2 Assessment Documentation Review

The initial step in performing the assessment is a document/procedure review. The PMTL will appoint one or more team member(s) to review the organization's SMS procedure/process documentation against the GAT. The PMT records the results of the documentation assessment and makes a recommendation regarding the documentation's acceptability to the PMTL, who conveys it to the PPL. The PMT will determine the documentation's acceptability. If the SMS procedure/process reviewed is not acceptable, the PMT will provide feedback to the organization regarding documentation areas of concern that need to be addressed. The organization and the FAA will repeat the submission and review cycle until the documentation is acceptable. The PMT will notify both the organization and the PMTL of all procedures/processes found acceptable.

11.1.3 Onsite Assessment Coordination

If the SMS procedure/process reviewed is acceptable, the PMTL, in consultation with the PMT, will determine if an onsite implementation assessment is needed. Then, if appropriate, the PMT will plan and initiate activities to perform an onsite assessment.

11.1.4 Conduct Assessment

Most of the assessment of an SMS implementation is expected to be conducted at the organization's facility/facilities as delineated in Section 6. However, in some circumstances a desk-top assessment may be performed against the D&M *SMS Framework* processes.

If the PMT finds the implementation acceptable, it will record its observations and supporting evidence/data and transmit recommendations to the PMTL, who conveys it to the PMTL. The PMT will determine the implementation acceptability. If the PMT approves the recommendation, the PMT records the assessment results and provides written acknowledgment to the company regarding the acceptability of the implemented procedure/process reviewed.

If the PMT finds the organization's SMS implementation unacceptable, it will record its observations and supporting information and transmit its recommendation to the PMTL, who conveys it to the PMT. The PMT then will provide written feedback to the company delineating areas of concern that need to be addressed. When a company accomplishes the SMS improvements needed, it should submit its information and request an updated assessment. The organization and the FAA will repeat the implementation assessment cycle until the implementation is found acceptable.

The PMT will notify both the organization and the PMTL of all implemented procedure/process found acceptable. The PMT will record the assessment results.

11.1.5 Letter of Acknowledgement

The PMT determines when the organization has met all the requirements for exiting a SMS Level and forwards its recommendation along with any supporting data to the PPL. The PMTL confirms that all exit criteria for the assessed Level have been satisfied and makes a recommendation to PMT for organization advancement.

Upon successful completion of each SMS Level, the PMT will provide a Letter of Acknowledgement for FAA management signature. The Letter will be signed by the appropriate Directorate Manager or the Director of Aircraft Certification Service or their designee. Then the FAA will send to the organization the "Letter of Acknowledgement," which attests to its participation in the SMS Pilot Project and the SMS Level achieved.

See Attachment 5 – Example Letter of Acknowledgement.

***Note*:** Participation in the SMS Pilot Project and the issuance of Letters of Acknowledgement do not constitute formal FAA acceptance or approval of individual SMS programs.

Assessment Process Overview

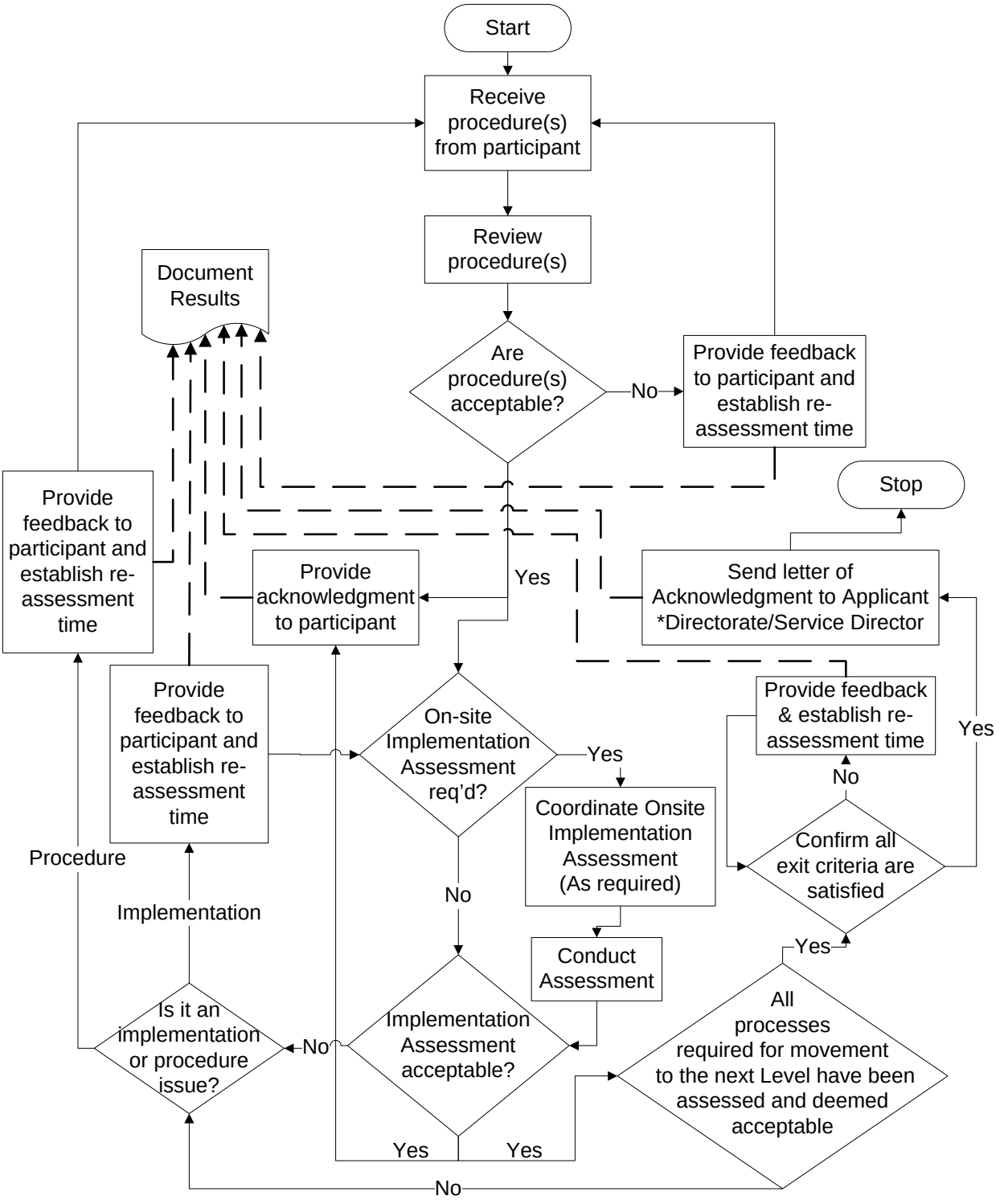


Figure 5: Assessment Process Overview

11.2 Documentation Assessment

The PMTL will select the PMT member(s) who will review the SMS documentation submitted by the organization. This assessment will determine the adequacy of the SMS documentation using the requirements outlined in the GAT and if it is found that:

1) The organization's SMS documentation is not sufficient, the PMTL recommends that the PMT provide feedback regarding its expectations;
2) The organization's SMS documentation is sufficient, the PMTL recommends the PMT provide an acknowledgment to the organization; and
3) The organization's SMS documentation is sufficient, the PMTL, in consensus with the PMT, will determine if an onsite assessment is warranted.

An integral part of the Pilot Project SMS assessment process will be assuring that the FAA meticulously documents and makes readily available to the organization the results of both the initial document review and subsequent onsite assessments of its SMS process. For each organization, the document assessment results will be recorded and maintained in a pilot project database.

The assessment will consist of two items:

1) Assessing the organization's SMS documentation with the GAT; and
2) Documenting materials to support consensus-building for establishment of a "Best Practices" repository into the out years as a means of continuously capturing and sharing the D&M industry's most robust SMS procedures.

11.2.1 SMS Documentation Sufficiency

The document assessment element requires reviewing the organization's SMS documentation for compliance with the GAT. The results will be documented in the GAT Assessment.

If the SMS documentation is found to be inadequate, the PMT will communicate its feedback and enable the organization to remedy any issues and resubmit its documentation. Once the organization's SMS documentation is accepted, the PMTL will notify the applicant and determine if an onsite assessment will be conducted (see Section 11.3 – Coordinate the Onsite Meeting).

The Pilot Project will begin capturing and recording the best practices during the documentation assessment and will work continuously to identify effective techniques and practices for implementing an SMS. These "Best Practices" will be verified and documented during onsite assessments recorded in the SMS Assessment database and summarized periodically. With appropriate safeguards for proprietary concerns and organization permission, this data will be made available to industry.

Once the PMT finishes reviewing the organization's submitted documentation, it will recommend to the PMTL whether an onsite implementation assessment is appropriate to verify the organization's implementation progress.

11.3 Coordinate the Onsite Meeting

Once the PMT determines that an onsite implementation assessment is appropriate it will notify the organization and coordinate with the organization to schedule the details of the assessment activities.

11.3.1 Onsite Assessment Scope

The duration and scale of the assessment must be determined based on the extent of organization's facilities and functions to be assessed so that the FAA can assign the proper personnel and allocate the necessary resources. The details for conducting an assessment are described in Section 11.4 – Conduct Onsite Implementation Assessment. Consideration will be given to the following:

1) SMS implementation Level (organization seeking to achieve Level 2 or 3),
2) Size of the organization/facility,
3) Complexity and criticality of the item being produced, and
4) Completeness of the documentation.

11.3.2 Notification to the Organization

Among the initial steps in planning an assessment will be to verify the proposed schedule and to identify the information that will be needed before commencing the assessment. Therefore, discussions between the PMTL and the appropriate company representative are expected prior to setting an assessment date. A written notification of intention to perform the assessment should then be sent to the organization. A sample format is provided in Attachment 4 – Sample Onsite Implementation Assessment Notification.

11.3.3 Modifications to Scheduled Assessments

Every effort will be made to maintain established assessment schedules. However, modifications to the schedule should be considered under special circumstances to meet the needs of either the FAA or the organization.

11.3.4 Unscheduled Assessments

Participation in this program is completely voluntary and no unscheduled evaluations will be conducted.

11.4 Conduct Onsite Implementation Assessment

11.4.1 General

The PMT members performing the implementation assessment should include the same individuals involved in the document assessment. Team members will receive briefing materials from the PMTL.

11.4.2 Team Makeup, Planning, and Schedule

The PMTL will post the assessment schedule, identifying the PMTL and PMT members. After the assessment has been coordinated with the organization, the PMTL will plan the assessment by:

1) Estimating the assessment duration, considering the organization in terms of:
    a) physical size of the facility,
    b) multiple locations/facilities,
    c) complexity of the organization's product,
    d) criticality of the organization's product (in terms of safety),
    e) number of different products,
    f) number of employees, example duration requirements might be:
        1. **small** facility with fewer than 50 total full-time persons: 1 to 2 days onsite;
        2. **medium** facility with 50 to fewer than 1000 total full-time persons: 2 to 3 days onsite; and
        3. **large** facility with 1000 or more total full-time persons: 3 to 5 days onsite;
2) Considering travel and lodging needs,
3) Coordinating number of assessment team members required with PMTL and, if using field personnel, verify their SMS experience;
4) Preparing a written assessment plan, including:
    a) Name and address of the organization,
    b) Assessment objectives,
    c) Dates of assessment,
    d) Names and contact information for the PMTL and PMT members; and
    e) Access information and the organization's POCs;
5) Coordinating assignments, requirements, and arrangements with team members as far in advance of the assessment as possible; notifying team members immediately of changes in schedule, assignments, requirements, and arrangements; and providing copies of all relevant organization documentation to team members.

11.4.3 SMS Assessment Preparation

The PMTL will coordinate with the designated representative of the organization to ensure that administrative arrangements for items such as team access, escorts, meeting rooms, and safety and security requirements are complete.

The PMTL and all team members will meet in advance of starting the assessment. During the Pilot Project, this meeting may take place at home station, by telecon, or at the organization's facility. They will review the following assessment elements, as appropriate, for proper coordination and common understanding:

1) Assessment Objectives and Plan,
2) Team functional assignments,
3) SMS Implementation Level,
4) SMS Implementation Plan, and
5) Any special guidance from the PMTL.

11.4.4 Pre-Assessment Conference

The PMTL will conduct a pre-assessment conference with appropriate organization management, cognizant supervisory personnel, and other appropriate personnel. At this meeting, as appropriate, the PMTL will:

1) Introduce team members and support service personnel;
2) Review the assessment's scope, objectives, and the conference agenda;
3) Discuss arrangements for the post-assessment conference;
4) Explain that the assessment is designed to ascertain the organization's progress in implementing its SMS; and
5) Allow time for a question-and-answer session.

11.4.5 SMS Implementation Assessment

The PMT will assess the implementation of the organization's SMS processes as defined in the assessment plan scope. The assessment will be based on the GAT. The PMT will perform the following tasks, as appropriate:

1) Review the organization's manuals, procedures, handbooks, policies, etc., to determine individual process implementation level. This can be accomplished by:
    a) Conducting desk review,
    b) Conducting personnel interviews, and
    c) Witnessing SMS processes in action, as implemented;
2) Determine if the organization is on schedule, per its Implementation Plan and document:
    a) Actual level of implementation versus organization stated level;
    b) Lessons Learned (Pluses (things that are great) and Deltas (things that could use improvement)); and
    c) Level of management support/commitment (subjective – have statement/facts to support);
3) Demonstrate SMS process(es) (if the SMS is mature enough during the assessment) to:
    a) Process an employee feedback;
    b) Performance of SRM process; and
    c) Performance of SA process.
4) The PMT member will document their assessment activities including:
    a) Individuals interviewed,
    b) Processes reviewed,
    c) Data reviewed, and
    d) Lessons Learned.

11.4.6 Assessment Meetings

1) The PMTL will hold daily meetings, as appropriate, with the PMT to:
    a) Review status of the assessment.
    b) Discuss problems encountered.
    c) Resolve any disagreements.
    d) Review plan for the next day's assessment.
    e) Discuss pluses and deltas captured during the day to ensure correctness, adequacy, and completeness.

The PMTL will ensure all Lessons Learned are recorded on the Assessment tool.

The PMTL also will hold meetings with the organization's representative(s) to discuss the progress of the assessment including issues encountered and the status of actions requested by the team, schedule changes, and the coordination of further assessment activities.

1) At the conclusion of the assessment, the PMTL will hold a final team meeting to:
    a) Resolve team disagreements on specific issues;
    b) Ensure all planned process areas were assessed;
    c) Discuss all issues and Lessons Learned to ensure that team members understand the items and can go forward in a coordinated manner with the PPL;
    d) Identify and record specific issues that the PMT believes have need of further action and share with the PMTL; and
    e) Discuss with team members, as appropriate, and record any Lessons Learned during the assessment that may improve future SMS policy or assessment techniques.

11.4.7 Post-Assessment Meeting

The PMTL will conduct a post-assessment meeting with the organization's management and cognizant supervisory personnel.

1) The PMTL, as appropriate, will:
    a) Introduce FAA personnel not previously introduced at the pre-assessment conference;
    b) Present preliminary assessment results including all issues and Lessons Learned;
    c) Explain that the results will be reviewed with the PMT and that a final report will be generated and provided to them;
    d) Encourage management to continuously provide lessons learned to the PMT;
    e) Encourage management to provide feedback on the conduct of the assessment by the FAA personnel;
    f) Request final comments and resolve any misunderstandings or disagreements before departure; and
    g) Ensure that the organization knows that results are not findings or demerits, but rather opportunities for improvement.

11.4.8 Recording Assessment Data

The PMTL will prepare the final assessment report for the PMT to review and approve. The PMTL will ensure that all copies of verification data are attached to the appropriate pluses and deltas (appropriately referenced and clearly identified) as part of the report. The report will be generated using Microsoft Word with all supporting data attached as a PDF file. The PMTL will record the approved report in SharePoint (for that organization). The PMTL for the assessment will provide the organization with a copy of the assessment final report along with either an acknowledgement for a successful assessment or a feedback request for issues found during the assessment.

11.4.9 Letter of Acknowledgement

At the successful completion of all Level 2 or 3 exit criteria, the PMTL will forward a notification letter and required documents to the PMTL acknowledging that the organization met all the requirements for promotion to the next Level. The PPL will prepare a Letter of Acknowledgement attesting to the organization's development of an SMS and its successful attainment of the appropriate SMS Level (Attachment 5 – Example Letter of Acknowledgement). The Aircraft Certification Service Director or their designee will sign the letter.

12 Overview of FAA's D&M SMS Oversight Process

The SMS may be documented in a form and manner that best serves the participant's need, however any modifications of existing FAA approved/accepted programs and their associated documents must be coordinated with the appropriate FAA oversight organization. The SMS Framework provides guidance for a participant to develop and document its SMS on a voluntary basis. A separate SMS manual is not required; however participants may find a separate SMS manual desirable while others may not.

After the participant has implemented an SMS the FAA will not conduct any oversight of their SMS unless an SMS rule applicable to D&M organizations is codified and the FAA has established an applicable oversight policy.

The FAA will recognize the policies and procedures assessed by the PMT during the pilot project for any future consideration of an SMS system if it becomes codified.

13 Comparison of Quality Assurance AS9100 versus SMS

A comparison of the two documents was conducted to determine which requirements are included in the SMS standards that are not fully present in the quality standard; a unidirectional comparison was studied by Embry-Riddle Aeronautical University. The results of the study can on the MSMS Sharepoint site.

14 Acronyms & Definitions

The MSMS team has developed the following set of definitions for select terms used in this Guide. The acronyms provided (following the definitions) are intended to clarify all acronyms used throughout D&M SMS pilot project documentation.

The following are the primary reasons for developing definitions for the selected terms:

1) Generic terms used – provide pointers to more specific types and context in guidance material;

2) Multiple words with similar meanings – clarified/differentiated in definitions; and

3) Terms that can be interpreted differently based on use and application – provide clarity on D&M meaning/application (e.g. Accident – is aligned with incident).

14.1 D&M SMS Pilot Project Definitions

Accident – An event that is unexpected, unforeseen, or unintended. Types of accidents include, but are not limited to: aircraft, industrial, and organizational.

In the context of SMS, specific use of the term "Accident" includes the following:

- Aircraft Accident – An occurrence associated with the operation of an aircraft that takes place between the time any person boards the aircraft with the intention of flight and all such persons have disembarked, and in which any person suffers death or serious injury, or in which the aircraft receives substantial damage (ref. 49 Code of Federal Regulations 830.2, Definitions, for the National Transportation Safety Board (NTSB), FAA Orders 8020.11 and VS8000.367); and
- Organizational Accident – Adverse consequences associated with an organization's structure, management, policies, processes, priorities, etc.

Accountability – The condition of being responsible for a process or a system's performance through the allocation and management of human, technical, financial, or other resources.

Analysis – The process of reviewing and/or studying data or information that typically leads to a decision or recommendation. The process can involve comparing information to criteria or a specific target measure, identifying trends, deficiencies, or root causes, and using scientific or mathematical methods.

In the context of SMS, specific uses of the term "Analysis" include the following:

- System Description and Analysis – process of identifying the scope of the system and system segments that will be used to define an organization's SMS
- Hazard Analysis – process of identifying hazards and evaluating the potential risk of a hazard
- Risk Analysis – process of quantitatively or qualitatively defining the likelihood and severity of a risk

Assessment – The process of evaluating or making a judgment against defined criteria to come to a conclusion or make a decision.

In the context of SMS, specific uses of the term "Assessment" include the following:

- Risk assessment – The process of determining the tolerability of risk associated with a hazard.
- System assessment – The process of determining if an organization conforms to its defined SMS and how effectively the SMS is performing.
- Gap Analysis (status) assessment – The process of determining the status for an expectation identified in the D&M *SMS Framework* during the Gap Analyses (Preliminary and Detailed).
- Implementation assessment – The process of determining the status for an expectation identified in the D&M *SMS Framework* once a company is in the process of implementing an SMS.

Audit – See "Internal Audit."

Authority – The capability to direct change, or control an organization's safety process or a segment of a system. In the context of SMS, it includes the capability to make decisions regarding risk acceptance and risk management.

Competency – An observable, measurable set of skills, knowledge, abilities, behaviors, and other characteristics that an individual needs to perform work roles of an occupation successfully. Competencies are typically required at different levels of proficiency depending on the work roles or occupational function. Competencies can help to ensure that individual and team performances align with the organization's mission and strategic direction.

Comply (Compliance) – To act in accordance with a request, demand, order, or rule (e.g. <*comply* with federal law>).

Component – One of the parts of a whole.

In the context of SMS, specific uses of the term "Component" include the following:

- A part of an aircraft; and,
- A major part of the D&M *SMS Framework*.

Conform (Conformity) – Act(ion) in accordance with some specified standard, practice, authority, etc.; a comparison of something to a document that describes it; agreement; accordance.

Control – See "Risk Control."

Corrective Action – Action to eliminate or mitigate the risk or reduce the effects of a detected nonconformity, a safety issue, or other undesirable situation.

Document – The written description of policies, processes, procedures, objectives, requirements, authorities, responsibilities, or work instructions (e.g., paper, electronic, etc.). It differs from *records*, which are the evidence of results achieved or activities performed.

Element (also Framework Element) **–** Each Framework Component is subdivided into "elements," which encompass the specific processes, tasks, or tools that the management system must engage or utilize in order to conduct the management of safety much like any other core business function or organizational process.

Evaluation – See "Internal Evaluation."

Function – A kind of action or activity performed by a person, an organization, equipment, or a combination thereof. In the context of SMS, "function" is used in the following manner:

- Safety-Related Function – A specific or discrete set of actions an organization performs to support or achieve a safety objective.
- Safety Assurance Function – The actions or activities an organization performs to fulfill the requirements of a Process and/or Element of the Safety Assurance Component.

Hazard – A condition that could foreseeably cause or contribute to an aircraft accident.

Incident – A minor event that may or may not lead to a more serious event.

In the context of SMS, specific uses of the term "Incident" include the following:

- An occurrence other than an accident associated with the operation of an aircraft, which affects or could affect the safety of operations (ref. 49 Code of Federal Regulations 830.2, Definitions, for the NTSB, FAA Orders 8020.11 and VS8000.367).

Interface – A common boundary or interconnection between two or more entities, which may be systems, equipment, organizations, concepts, or human beings. In the context of SMS, an interface may be found between organizations, work units, employees, systems, processes, and procedures.

Internal Audit – Scheduled formal reviews and verifications that determine if an organization has complied with its defined policy, standards, and/or contract requirements. In the context of SMS, an "Internal Audit" is differentiated from an "Internal Evaluation," as the former is typically focused on "conformance" rather than "performance."

Internal Evaluation – An independent review of organization policies, procedures, and systems. An evaluation may be an anticipatory process designed to identify and correct potential problems before they happen. In the context of SMS, an "Internal Evaluation" is differentiated from an "Internal Audit," as the former is typically focused on "performance" rather than "conformance."

Lessons Learned – Knowledge or understanding gained by experience, which may be positive, such as a successful test or mission, or negative, such as a mishap or failure.

Life Cycle – The time between conception, through development, design and manufacture (or implementation), through service and to disposal.

In the context of SMS, specific use of the term "Life Cycle" includes the following:

- System Life Cycle **–** Within the boundaries that define an organization's system, the integration of people, data, processes, and business systems that are designed to advance an organization's enterprise and how it performs over time.

Likelihood – The estimated probability or frequency, in quantitative or qualitative terms, of an occurrence.

Management – The person or group of people who direct and control an organization. This term is intended to include all levels of management. Use of the term "Management" is used to differentiate from those individuals who are employees and carry out direction and execute controls.

Objective – The desired state or performance target of an organization or process.

See "Safety Objective" for the specific use of the term in the context of SMS.

Operations – The performance of the business functions and systems that contribute to an organization's creation of outputs (includes design, parts, components, and aircraft products, etc.).

In the context of SMS, the term is used as defined above. Other uses, such as an organizational reference or type of activity (e.g. operations can sometimes refer to the portion of an aircraft life cycle) are not intended as it pertains to the D&M *SMS Framework*.

Organization – Within the context of this document, the term *organization* refers to any aviation design and manufacturing operation.

Outputs – The product or end result of a process or activity, which is able to be recorded, monitored, measured, and analyzed.

See "SMS Outputs" for the specific use of the term in the context of SMS.

Oversight – A function performed by a regulator (such as the FAA) that ensures that an organization complies with and uses safety-related standards, requirements, regulations, and associated procedures. Safety oversight also works to assure that the acceptable level of safety risk is not exceeded in the air transportation system.

Preventive Action – Preemptive action to eliminate or mitigate the potential cause or reduce the future effects of an identified unsafe condition or anticipated nonconformity or other undesirable situation.

Probability – The ratio of the number of actual occurrences to the number of possible occurrences (e.g., 1 in 1 million flight hours). Probability is often expressed with the denominator normalized to a single unit (e.g., $1x10^{-6}$ per flight hour) or as a percent. Use of the term probability is generally limited to quantitative calculations of risk. See "Likelihood," which is a more general term used in the determination of risk (implying the potential for qualitative determinations, as well as, quantitative).

Procedure – Specified ways to carry out operational activities that translate the *what* (objectives) into *how* (practical activities). Procedures are often considered to be the documented "step-by-step" detail of a process.

Process – A set of interrelated or interacting activities that transform inputs into outputs.

Product – A tangible outcome or output of a process or activity. In the context of SMS, "Product" refers to an output of a process or system that an aviation organization offers for purchase.

In some FAA organizations, the use of the term "Product" is intended to refer to an aircraft, engine, or propeller only. In the context of the D&M SMS Framework, the intent is for the term to refer to *anything* the organization produces.

Records – Evidence of results achieved or activities performed (also see *Document* above).

Responsibility – The obligation or duty to manage or execute specific activities. Typically, a responsibility is an activity that has been assigned or delegated from a higher level authority.

Risk – The composite of predicted severity (how bad) and likelihood (how probable) of the potential effect of a hazard. The terms *risk* and *safety risk* are interchangeable for the purposes of this document.

Risk Control – Steps taken to eliminate (remove) hazards or to mitigate (lessen) their effects by reducing the severity and/or likelihood of risk associated with those hazards.

Safety Culture – The product of individual and group values, attitudes, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of, the organization's management of safety. Organizations with a positive safety culture are characterized by communications founded on mutual trust, shared perceptions of the importance of safety, and confidence in the efficacy of preventive measures.

Safety Management Plan – A defined and systematic approach to risk management that addresses the people, policies, procedures, tasks, resources, and communications needed to achieve stated safety objectives of an organization's SMS.

Safety Objective – A goal or desirable outcome related to safety. Generally, it is based on the organization's safety policy, and specified for relevant functions and levels in the organization. Safety objectives are typically measurable.

Safety-Related Function – See "Function."

Safety-Related Position(s) – A position with defined responsibility(ies) for an aspect of organizational or product safety that supports or achieves a safety objective.

Safety Risk – See "Risk."

Safety Risk Control – See "Risk Control."

Severity – The degree of loss or harm resulting from a hazard.

SMS Outputs – The product or end result of an SMS process, which is able to be recorded, monitored, measured, and analyzed. Outputs are the minimum expectation for the product of each process area and the input for the next process area in succession.

Substitute Risk – A risk unintentionally created as a consequence of safety risk control(s).

System – An integrated set of constituent elements that are combined in an operational or support environment to accomplish a defined objective. These elements include people, hardware, software, firmware, information, procedures, facilities, services, and other support facets.

System Segment – A generic term for a portion (and all its constituent parts) of a system.
In the context of the D&M SMS Pilot Project, "System Segment" refers to the major parts of an organization's SMS system description. System Segments are specifically used in the Preliminary Gap Analysis, Detailed Gap Analysis, Implementation Plan, Assessment tools to compartmentalize an organization into more manageable parts for the purpose of conducting an assessment.

Top Management – The person or group of people that directs/controls an organization and is responsible for its success or failure.

14.2 D&M SMS Pilot Project Acronyms

AC – Advisory Circular

ACO – Aircraft Certification Office

ACSEP - Aircraft Certification Systems Evaluation Program

AD – Airworthiness Directive

AE – Accountable Executive

AIR – Aircraft Certification Service

ARC – Aviation Rulemaking Committee

ASAP – Aviation Safety Action Program

ASE – Aviation Safety Engineer

ASI – Aviation Safety Inspector

ASQ – American Society for Quality

AVS – Aviation Safety

CAD – Computer Aided Design

CASS – Continuing Analysis and Surveillance System

CFR – Code of Federal Regulations

CM – Certificate Management

CMO – Certificate Management Office

DOT – U.S. Department Of Transportation

D&M – Design and Manufacturing

FAA – Federal Aviation Administration

FAQ – Frequently Asked Questions

FMEA – Failure Modes and Effects Analysis

FOIA – Freedom of Information Act

FOQA – Flight Operational Quality Assurance

FSDO – Flight Standards District Office

GAT – Gap Analysis Tool

HAZ – Hazard

ICAO – International Civil Aviation Organization

IP3 – Integrated Pilot Project Plan

ISO – International Organization for Standardization

LAACO – Los Angeles Aircraft Certification Office

MIDO – Manufacturing Inspection District Office

MISO – Manufacturing Inspection Satellite Office

MSMS - Manufacturers Safety Management System

NPRM – Notice of Proposed Rulemaking

NTSB - National Transportation Safety Board

OnE – Oversight and Evaluation

PAH – Production Approval Holder

PC – Production Certificate

PI – Principal Inspector

PMA – Parts Manufacturer Approval

PMT – Participant Management Team

PMTL – Participant Management Team Lead

POC – Point of Contact

PPL – Pilot Project Lead

P&P – Policy and Procedure

QA – Quality Assurance

QMS – Quality Management System

SA – Safety Assurance

SAE – Society of Automotive Engineers

SMS – Safety Management System

SRM – Safety Risk Management

STC – Supplemental Type Certification

TC – Type Certificate

TBD – To Be Determined

TSO – Technical Standard Order

TSOA – Technical Standard Order Authorization

VDRP – Voluntary Disclosure Reporting Program

15 References

1) D&M SMS Gap Analysis Tool file
(file name: “SMS Gap Analysis_CompanyName_MMDDYY_21DEC2010.xls”) – Overview information and instructions are provided on the first tab;

2) Developmental Guidance for D&M SMS
(file name: “Developmental Guidance for D&M SMS DDMMMYY.doc”);

3) Design and Manufacturing *SMS Framework*, Revision A, dated 13th January 2011;

4) Safety Management Systems for Part 121 Certificate Holders Notice of Proposed Rulemaking (14 CFR Parts 5 and 119, Docket No. FAA–2009–0671) – Federal Register Volume 75, No. 214, page 68242; Friday, November 5, 2010;

5) International Civil Aviation Organization (ICAO) *SMS Framework* – Annex 6 to the Convention on International Civil Aviation, Operation of Aircraft, Appendix 7 – Framework for Safety Management Systems (SMS) (see also Chapter 3, 3.3.4 and Chapter 8, 8.7.3.4), (http://www2.icao.int/en/ism/ICAO%20Annexes/Annex%206.pdf);

6) ICAO Safety Management Manual (SMM), Second Edition, 2009 – Document 9859, (http://www.icao.int/anb/safetymanagement/DOC_9859_FULL_EN.pdf);

7) FAA Order 8000.369, Safety Management System Guidance, Effective Date: 09-30-2008, (http://www.faa.gov/documentLibrary/media/Order/8000.369.pdf);

8) FAA Order VS 8000.367, Aviation Safety (AVS) Safety Management System Requirements (Appendix B: Product/Service Provider SMS Requirements), Effective Date: 05-14-2008, (http://www.acsf.aero/attachments/wysiwyg/12/FAA_ORDER_VS8000.367_SMS_Requirements.pdf);

9) Transport Canada, Introduction to Safety Management Systems, TP 13739, 04/2001, (http://www.tc.gc.ca/publications/BIL/TP13739/PDF%5CHR/TP13739b.pdf);

10) International Civil Aviation Organization (ICAO): Statement on amendments to Annex 8 of the Convention on International Civil Aviation, Operation of Aircraft (http://www.paris.icao.int/news/200906_amendments_to_annexes_annex8.htm);

11) Manuele, Fred A., On the Practice of Safety, John Wiley & Sons, 2003, Hoboken, NJ.

12) 49 Code of Federal Regulations 830.2, Definitions, for the NTSB, FAA Orders 8020.11 and VS8000.36.

APPENDIX A: D&M SMS Framework

The information included in Appendix A was extracted from:

Design and Manufacturing (D&M) *SMS Framework*, Revision B, dated October 13, 2011.

Component 1.0 Safety Policy and Objectives

The organization will develop and implement an integrated, comprehensive SMS for its entire* organization and will incorporate a procedure to identify and maintain compliance with current safety-related legal and regulatory requirements. The safety policy shall be periodically reviewed to ensure it remains relevant and appropriate to the organization. Final approval will be based on approval from the Top Management representative.

**Entire organization participating within the scope of the pilot project*

Element 1.1 Safety Policy

Top Management will define the organization's safety policy and convey its expectations and objectives to its employees.

1) Top Management will define and sign the organization's safety policy;
2) The safety policy will:
    a) Include a commitment to implement, maintain, and improve the SMS;
    b) Include a commitment to identify and comply with legal and regulatory requirements;
    c) Include a commitment to encourage employees to report safety issues without reprisal (as per Sub-Element 3.1.5);
    d) Establish clear standards for acceptable operational behavior for all employees;
    e) Provide management guidance for setting safety objectives;
    f) Provide management guidance for reviewing performance according to the organization's safety objectives;
    g) {Paragraph removed – duplication}
    h) Be communicated with visible management endorsement to all employees and responsible parties;
    i) Be reviewed periodically to ensure it remains relevant and appropriate to the organization;
    j) Identify responsibility and accountability of management and employees with respect to the organization's safety objectives;
    k) *{Paragraph removed – duplication}*
    l) *{Paragraph removed – duplication}*
3) *{Paragraph Moved to DG}*
4) *{Paragraph Moved to DG}*
5) *{Paragraph Moved to DG}*

Element 1.2 Management Commitment and Safety Accountabilities

Management will define, document, and communicate the safety roles, responsibilities, and authorities throughout its organization.

1) The organization will appoint an accountable executive that will have the ultimate accountability for the SMS;
2) Top Management will provide resources essential to implement and maintain the SMS;
3) *{Paragraph removed – duplication}*Aviation safety-related positions, responsibilities, and authorities will be:
    a) *{Paragraph removed – duplication}*
    b) *{Paragraph Moved to DG}*
    c) *{Paragraph Moved to DG}*
4) The organization will define levels of management that can make safety risk acceptance decisions as described in Element 2.2(2);
5) *{Paragraph Moved to DG}*

Element 1.3 Designation and Responsibilities of Required Safety Management Personnel

1) The organization must identify an Accountable Executive who, irrespective of other functions, satisfies the following:
    a) Is the final authority over operations associated with the organization's certificate/approval(s);
    b) Controls the financial resources required for the operations associated with the organization's certificate/approval(s);
    c) Controls the human resources required for the operations associated with the organization's certificate/approval(s);
    d) Retains ultimate responsibility for the safety performance of the operations associated with the organization's certificate/approval(s).
2) The Accountable Executive must accomplish the following:
    a) Ensure that the SMS is properly implemented and performing in all areas of the organization;
    b) Develop and sign the safety policy of the organization;
    c) Communicate the safety policy throughout the organization;
    d) Regularly review the organization’s safety policy to ensure it remains relevant and appropriate;
    e) Regularly review the safety performance of the organization and direct actions necessary to address substandard safety performance in accordance with Sub-Element 3.1.8.
3) The Accountable Executive must designate a management representative who, on behalf of the Accountable Executive, must be responsible for the following:
    a) *{Paragraph Moved to DG}*
    b) Facilitating hazard identification and safety risk analysis;
    c) Monitoring the effectiveness of safety risk controls;
    d) Ensuring safety promotion throughout the organization per Component 4.0;
    e) Regularly reporting to the Accountable Executive on the performance of the SMS and on any need for improvement.

Element 1.4 Emergency Preparedness and Response

The organization will develop and implement procedures, as necessary that it will follow in the event of an accident or incident.

Element 1.5 SMS Documents and Records

The organization will develop and maintain documentation that describes the organization's safety policy and SMS processes and procedures.

The organization will:

1) Maintain records of outputs of safety risk management and safety assurance processes for as long as the affected aircraft, engine, propeller, or article remains in service;
2) Maintain records of all training provided and a list of trained individuals, as required under Sub-Element 4.1.2, for a minimum of 24 consecutive calendar months after training completion;
3) Retain records of all safety information communication for a minimum of 24 consecutive calendar months.

Component 2.0 Safety Risk Management (SRM)

The organization will develop processes to determine the critical characteristics of its systems and operational environment and apply this knowledge to identify hazards, analyze and assess risk, and design risk controls.

Element 2.1 Hazard Identification and Analysis

1) The SRM process will be applied to:
    a) Initial designs of systems, organizations, and/or products; and the operation and maintenance of these systems, organizations, and/or products;
    b) The development of D&M processes and procedures;
    c) New or recurring hazards that are identified in the Safety Assurance functions (described in Element 3.1), including information collected during design, manufacturing, operation and maintenance, etc; and
    d) Planned changes to D&M processes, including product, component, or part design changes, maintenance and operation instructions, and assumptions when a design is developed.

Sub-Element 2.1.1 System Description and Analysis

The organization will analyze its systems, operations, and operational environment to gain an understanding of critical design and production performance factors, processes, and activities to identify hazards.

1) A system description and analysis will be developed to the level of detail necessary to identify hazards and implement risk controls.

Sub-Element 2.1.2 Identify Hazards

The organization will identify and document the hazards in its operations that are likely to cause death, serious physical harm, or damage to equipment or property in sufficient detail to determine associated level of risk and risk acceptability. The organization will identify hazards for both the products they produce and the processes conducted by the organization.

1) Hazards will be:
    a) Identified for the scope of the system, as defined in the system description[5], and
    b) *{Paragraph removed – duplication}*
2) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*

Element 2.2 Risk Assessment and Control

1) *{Paragraph Moved to DG}.*
2) The organization will develop a risk acceptance process;
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
    c) *{Paragraph Moved to DG}*
        1. *{Paragraph Moved to DG}*
        2. *{Paragraph Moved to DG}*
    d) *{Paragraph removed – duplication}*
    e) *{Paragraph Moved to DG}*
3) The organization will establish feedback loops from assurance functions described in Component 3.0 to evaluate the effectiveness of safety risk controls.

Sub-Element 2.2.1 Analyze Safety Risk

The organization will determine and analyze the severity and likelihood of potential consequences associated with identified hazards and will identify contributing factors.

1) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
    c) *{Paragraph Moved to DG}*
    d) *{Paragraph Moved to DG}*
        1. *{Paragraph Moved to DG}*
        2. *{Paragraph Moved to DG}*

Sub-Element 2.2.2 Assess Safety Risk

The organization will assess risk associated with each identified hazard and define risk acceptance procedures and levels of management that can make safety risk acceptance decisions.

[5] While it is recognized that identification of every conceivable hazard is impractical, organizations are expected to exercise due diligence in identifying and controlling significant and reasonably foreseeable hazards related to their operations.

1) Each hazard will be assessed for its safety risk acceptability using the safety risk acceptance process described in Element 2.2(2).

Sub-Element 2.2.3 Control/Mitigate Safety Risk

The organization will design and implement a safety risk control for each identified hazard for which there is an unacceptable risk, to reduce risk to acceptable levels.

1) *{Paragraph removed – duplication}*
2) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
    c) *{Paragraph Moved to DG}*
    d) *{Paragraph Moved to DG}*
3) *{Paragraph Moved to DG}*

Component 3.0 Safety Assurance (SA)

The organization will monitor, measure, and evaluate the performance of risk controls.

Element 3.1 Safety Performance Monitoring and Measurement

1) The organization will monitor their systems and operations to:
    a) Identify new and recurring hazards,
    b) Measure the effectiveness of safety risk controls,
    c) Ensure compliance with regulatory requirements.
2) The organization will collect the data necessary to demonstrate the effectiveness of its systems and operations.

Sub-Element 3.1.1 Continuous Monitoring

The organization will monitor data throughout the lifecycle, including those associated with components and services received from suppliers and contractors, to identify hazards, measure the effectiveness of safety risk controls, and assess system performance.

1) *{Paragraph removed – duplication}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
    c) *{Paragraph Moved to DG}*
    d) *{Paragraph Moved to DG}*

Sub-Element 3.1.2 Internal Audit

The organization will conduct internal audits of the SMS to determine if the SMS conforms to the organization's processes and procedures.

1) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
2) *{Paragraph Moved to DG}*
3) *{Paragraph Moved to DG}*

Sub-Element 3.1.3 Internal Evaluation

The organization will perform regularly scheduled internal evaluations of its systems and operations to determine the performance and effectiveness of risk controls. The scope of evaluations must include:

1) *{Paragraph Moved to DG}*
2) *{Paragraph Moved to DG}*

Sub-Element 3.1.4 Investigation

The organization will establish procedures to collect data to investigate instances of potential regulatory noncompliance and to identify potential new hazards or risk control failures.

Sub-Element 3.1.5 Employee Reporting and Feedback System

The organization will actively use an employee safety reporting and feedback system.

1) *{Paragraph Moved to DG}*
2) Employees will be encouraged to submit solutions/safety improvements.
3) *{Paragraph Moved to DG}*
4) *{Paragraph Moved to DG}*
5) Employees will be allowed confidentiality when using the employee safety reporting and feedback system.

Sub-Element 3.1.6 Analysis of Data

The organization will analyze the data acquired in Sub-Elements 3.1.1 through 3.1.5 to assess the performance and effectiveness of risk controls in the organization's systems and operation.

1) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
    c) *{Paragraph Moved to DG}*
    d) *{Paragraph Moved to DG}*

Sub-Element 3.1.7 System Assessment

The organization will assess the safety performance and effectiveness of risk controls, its ability to achieve the organization's safety objectives and its conformity to the design of the organization's SMS.

1) The organization will assess the performance of:
    a) Risk controls put in place by the organization for their effectiveness,
    b) Safety-related functions of the design and production-related processes against its objectives and expectations,
    c) The SMS against its objectives and expectations.
2) The organization will use the information obtained under Sub-Element 3.1.6 and from other sources as necessary, to make their assessments.
3) System assessments will document results that indicate a finding of:
    a) Conformity with existing safety risk control(s)/the organization's SMS expectations(s) (including regulatory requirements applicable to the SMS);

b) Nonconformity with existing safety risk control(s)/the organization's SMS expectations(s) (including regulatory requirements applicable to the SMS); and
c) New hazards found and how the organization will deal with them.

4) *{Paragraph Moved to DG}*
5) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
        1. *{Paragraph Moved to DG}*
        2. *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
        1. *{Paragraph Moved to DG}*
        2. *{Paragraph Moved to DG}*
    c) *{Paragraph Moved to DG}*
    d) *{Paragraph Moved to DG}*
6) The SRM process will be utilized if the analysis of data from Sub-Element 3.1.6 indicates:
    a) The identification of new or potential hazards, or
    b) The need for system changes.
7) *{Paragraph removed – duplication}*

Sub-Element 3.1.8 Management Review

As part of their commitment to continual improvement, Top Management will conduct annual reviews of the SMS, at a minimum. Management reviews will include assessing the performance and effectiveness of the organization's systems and operations and the need for improvements.

1) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
    c) *{Paragraph Moved to DG}*
    d) *{Paragraph Moved to DG}*
2) *{Paragraph Moved to DG}*
3) *{Paragraph Moved to DG}*
4) Top Management will maintain records of the reviews and the findings in accordance with Element 1.5.

Element 3.2 Management of Change

The organization will identify and assess safety risk for changes arising within or external to the organization that may affect established systems or operations. These changes may be to existing system designs, new system designs, or new/modified operations or procedures.

1) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
2) *{Paragraph Moved to DG}*

Component 4.0 Safety Promotion

Top Management will promote the growth of a positive safety culture and communicate it throughout the organization.

Element 4.1 Competencies and Training

Sub-Element 4.1.1 Personnel Expectations (Competence)

The organization will document SMS competency requirements for those positions identified in Elements 1.2(3) and 1.3 and ensure those requirements are met.

1) *{Paragraph Moved to DG}*
2) *{Paragraph Moved to DG}*

Sub-Element 4.1.2 Training

The organization will develop and maintain a safety training program that ensures personnel are trained and competent to perform their role within the SMS. The organization will also regularly evaluate training necessary to meet competency requirements of Sub-Element 4.1.1(1).

1) *{Paragraph Moved to DG}*
2) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*

Element 4.2 Communication and Awareness

{Paragraph Moved to DG}

1) Top Management will communicate to the organization, at a minimum, the following information:
    a) Rationale behind decisions to implement controls, preventive actions, corrective actions;
    b) Rationale behind decisions to not take action;
    c) *{Paragraph Moved to DG}*
    d) *{Paragraph Moved to DG}*
2) Top Management will make SMS information readily accessible to anyone in the organization that will use it corresponding to their safety-related role/responsibility(ies).
3) The organization will provide the FAA ready access to the outputs of the SMS.
4) *{Paragraph Moved to DG}*
5) *{Paragraph Moved to DG}*
6) *{Paragraph Moved to DG}*
    a) *{Paragraph Moved to DG}*
    b) *{Paragraph Moved to DG}*
        1) *{Paragraph Moved to DG}*
        2) *{Paragraph Moved to DG}*
        3) *{Paragraph Moved to DG}*
        4) *{Paragraph Moved to DG}*
        5) *{Paragraph Moved to DG}*
        6) *{Paragraph Moved to DG}*

D&M SMS Framework Change and Revisions Log

Revision #	Date	Pages/Section Affected	Description of Revision
A	1/13/2011	a) 16/Element 3.1(1)(c); b) 16/Sub-Element 3.1.2; c) 18/Sub-Element 3.1.7; d) 19/Element 3.2	a) Formatting b) Word change c) Word change d) Sentence deleted
B	10/13/2011	All sections	Revised to identify content moved to Developmental Guidance and deletion of duplicate expectations.

APPENDIX B: D&M SMS Pilot Project Levels

Implementation Level 1: Planning and Organization

Level 1 Objectives

1) Complete a preliminary and detailed gap analyses; and
2) Complete a comprehensive implementation plan that addresses closing the gaps identified in the detailed gap analysis. (reference paragraph 6.3.4)

Level 1 Activity

Level 1 activities are designed to plan, organize, and prepare the organization for SMS development. The level 1 activities should be within the defined scope of the SMS system description. During the Gap analysis and implementation planning an organization may choose to change or expand the scope of their SMS implementation for the pilot project. Prior coordination with the PMT is essential for any change in scope as this could affect the objectives of the SMS pilot project.

Level 1 Input

The decision of an organization's top management team to commit to voluntary implementation of an SMS and participation in the SMS Pilot Project begins the SMS Level 1 implementation process. The necessary input of guidance, objectives, and expectations for Level 1 implementation efforts will be provided prior to the Orientation Meeting and further discussed during the Orientation Meeting.

Level 1 Output

While no actual development activities are expected during Level 1, beyond those listed in the *SMS Framework*, Elements 1.1, 1.2 (partial), 1.3 and 4.1.1 (partial), the following items are to be accomplished prior to Level 1 exit:

1) Data showing top management's commitment to implement SMS, define safety policy, and convey safety expectations and objectives to its employees (*SMS Framework* Element 1.1; "Safety Policy");
2) Data showing top management's commitment to ensure adequate resources are available to implement SMS (in accordance with *SMS Framework* Element 1.2(2) Management Commitment & Safety Accountabilities;
3) Designation of a management representative who will be responsible for SMS development (*SMS Framework* Sub-Element 1.3(1); "Key Safety Personnel");
4) Completed preliminary and detailed gap analyses on the entire* organization for all elements of the *SMS Framework* (APPENDIX A: D&M SMS Framework);
5) Completed comprehensive SMS implementation plan for all elements to take the organization through Level 4 (APPENDIX C: Tools and Templates); and
6) Identified safety competencies necessary in accordance with *SMS Framework* Sub-Element 4.1.1 Personnel Expectations (Competence), and develop a training plan

commensurate with Level 1 implementation phase of maturity for those competencies, for all employees participation within the scope of the system description (in accordance with *SMS Framework* Sub-Element 4.1.2 Training).

Level 1 – Output Documents

1) Safety Policy;
2) Detailed Gap analysis
3) Comprehensive SMS implementation plan (Summary) for the entire* organization through SMS Implementation Level 4 (within the scope of the system description); and
4) SMS Training Plan for all employees (employees participating within the scope of the system description).

The Level 1 Exit Criteria Worksheet is included as Attachment 1 **– Level 1 Exit Criteria Worksheet**. This worksheet is used by the PMT to establish when a participant can proceed to the next level within the system description. The worksheet includes the outputs and output documents listed above. The exit criteria worksheet is not intended to hold a participant from implementing any part of an SMS system at any time. The worksheet aids the PMT and the participant to progress from one level of maturity to the next and standardizes the implementation of an SMS during pilot project development.

Implementation Level 2: Reactive Process, Basic Risk Management

Level 2 Objective

The objective of Level 2 is to correct **known** deficiencies in safety management practices and operational processes.

Note: These known deficiencies may be based on a variety of sources including past inspection and audit reports, accident and incident investigations, and employee reports, among others.

The organization will plan, organize, and prepare the organization for further SMS development. This will include complying with the elements in the D&M *SMS Framework*:

Level 2 Input

The outputs, documentation, detailed gap analysis, and implementation plan from the Level 1 exit process will provide the initial input for Level 2 development.

Additional input includes results from:

1) Previous internal and external audit reports and evaluations,
2) Accident and incident investigations, and
3) Employee reports and/or feedback.

Consider input from existing data sources such as:

1) Warranty returns reports
2) Service difficulty reports
3) Airworthiness directives
4) Special/alert service bulletins
5) Financial data

Level 2 Process Overview

At this step, the organization develops and implements basic safety risk management and safety assurance processes. Information acquisition, processing, and analysis functions are implemented and a tracking system for risk control and corrective actions is developed. This allows the organization to systematically address known problems and react to newly identified problems as they occur and to develop appropriate remedial action.

At the end of Level 2, most of the essential safety management structure and basic identification, analysis, and assessment functions of an SMS will be in place, however because the forward looking systems and task analyses have not yet been conducted, the system is still functioning at a reactive level. For this reason, this level is termed ‘reactive.’ While this is not the final objective of an SMS, it is an important step in the evolution of safety management capabilities.

Also in this level the PMT will assess processes and procedures per paragraph Part C of this guide.

Level 2 Procedures

During the Level 2 implementation phase, the organization will:

1) Develop basic safety information management and analytical processes,
2) Identify, analyze, and assess known hazards,
3) Design and implement risk controls,
4) Develop basic safety assurance and analytical processes, to include management reviews,
5) Develop non-punitive voluntary employee reporting system, and
6) Identify, document and complete necessary training relevant to SMS implementation at Level 2.

Level 2 Output

The documentation and performance desired for Level 2 exit status assessment are listed below:

1) Documented processes and procedures for operating the SMS to the level of reactive analysis, assessment, and mitigating actions;
2) Develop documentation relevant to SMS implementation plan and SRM components (reactive processes)
3) Initiated and documented voluntary non-punitive employee reporting and feedback program;
4) Conducted SMS training for the staff directly involved in the SMS process to at least the level necessary for the SMS reactive processes;
5) Applied SRM processes and procedures to at least one known (existing) hazard and initiate the mitigation process to control/mitigate the risk associated with the hazard;
6) Updated the detailed gap analysis on the entire* organization for all elements of the *SMS Framework*; *(within the scope of the system description)* and
7) Updated the comprehensive SMS implementation plan for all elements to take the organization through Level 4. *(within the scope of the system description)*

Level 2 Output Documents

Documentation for the following (elements and processes implemented during Level 1 have already been documented and need not be repeated for Level 2):

1) Data showing that SRM processes and procedures have been applied to at least one existing hazard and that the mitigation process has been initiated.
2) Updated comprehensive SMS implementation plan for all elements to take the organization through Level 4 (within the scope of the system description);

3) Updated SMS Training Plan for all employees (employees participating within the scope of the system description).

Once the process and procedural items listed above have been completed, there will a joint assessment of the status of the organization's SMS development. The organization will present

their progress (to include updated and current detailed gap analysis and implementation plan) to their PMT and the PPL prior to proceeding to Level 3.

In conducting the document review and assessment, it should be noted that the objective is to develop and implement the specific processes and procedures necessary for applying SMS reactively for the systems listed in the *SMS Framework*, Element 1.1 (3), as appropriate.

The Level 2 Exit Criteria Worksheet is included as Attachment 2 – Level 2 Exit Criteria Worksheet. This worksheet is used by the PMT to establish when a participant can proceed to the next level within the pilot project. The worksheet includes the outputs and output documents listed above. The exit criteria worksheet is not intended to hold a participant from implementing any part of an SMS system at any time. The worksheet aids the PMT and the participant to progress from one level of maturity to the next and standardizes the implementation of an SMS during pilot project development.

Implementation Level 3 – Proactive Processes, Looking Ahead – A Fully Functioning SMS

Introduction

Element 2.1 (1) of the *SMS Framework* expects Safety Risk Management (SRM) to be applied to initial design of systems, organizations, and products and to the operation and maintenance of these; development of D&M procedures; new or recurring hazards identified; and planned changes to D&M procedures. The activities that make up the SRM process involve careful analysis of systems and tasks, identification of potential hazards in these functions, and development of risk controls. The risk management process developed at Level 2 is used to analyze, document, and track these activities. At this level, the organization is now using the processes to look ahead; this level is called "proactive." At this level, however, these proactive processes have been implemented but their performance has not yet been proven.

The organization will develop processes to understand the critical characteristics of its systems and operational environment and apply this knowledge to the identification of hazards, risk decision making, and the design of risk controls.

Level 3 Objective

The first overall objective of SMS development is captured in the first objective of the policy component of the *SMS Framework*:

"The organization will develop and implement an integrated, comprehensive SMS for its entire organization."*

The specific objective of Level 3 is to develop processes to understand the critical characteristics of its systems and operational environment and apply this knowledge to the identification of hazards, risk decision making, and the design of risk controls. This will include complying with the following expectations in the *SMS Framework*:

1) Demonstrated performance of Level 2 Expectations;
2) Data showing that the processes are being updated, maintained, and practiced;

3) Apply the SRM process to all Element 2.1 (1)(a), (b) & (d) items;
4) Comply with Process 2.1.1;
5) Comply with Element 3.2;
6) Comply with Element 4.1;
7) Apply the SRM processes and procedures to at least one existing hazard and initiate the mitigation process; and
8) Complete all SMS staff and employee training commensurate with this level of implementation phase maturity.

Level 3 Input

The outputs, documentation, and implementation plan from the Level 2 exit process will provide the initial input for Level 2 development. Additional input includes results from Internal Evaluation Program, Warranty Return and Quality Escape Programs, Continued Operational Safety Program (COS), Reliability and Maintainability Programs, previous internal and external audit reports, accident and incident investigations, and employee reports.

References

1) D&M *SMS Framework*, as revised.

Level 3 Procedure

During the Level 3 implementation phase, the organization will:

1) Implement SRM for proactive and predictive processes.
    a) Initial designs of systems, organizations, and/or products;
    b) The development of operational procedures; and
    c) Planned changes to the operational processes.

2) System and task descriptions will be developed to the level of detail necessary to:
    a) Identify hazards;
    b) Develop operational procedures; and
    c) Develop and implement risk controls.

3) Perform training relevant to proactive and predictive processes.
    a) Personnel Competency and Training.

4) Develop documentation relevant to proactive and predictive processes.
    a) SMS Implementation Plan, and
    b) SMS Documentation.

5) Incorporate identified hazards from System and Task Analyses into SRM process.

6) Refine safety information management and analytical processes to incorporate proactive safety management processes for:
    a) Information acquisition,
    b) Analysis of data,
    c) System assessment,
    d) Preventive and corrective actions, and
    e) Management reviews.

7) Initiate policy and procedures for:
    a) Management of Change, and
    b) Continual Improvement.

8) Complete training of all employees commensurate with the Level 3 implementation phase of maturity.

Level 3 Output

Completion Criteria

Once the objectives and procedures outlined above have been completed, there will be a joint assessment of the status of SMS development by the organization, the PMT, and the PPL before proceeding to Level 4. The documentation and GAT used for Level 3 status assessment are listed below. In conducting the document review and assessment, it should be noted that the objective is to develop and implement the full capabilities necessary for applying SMS.

Assessment Criteria

The organization must have accomplished at least the following:

1) Demonstrated performance of Level 2 expectations;
2) Data showing that all SMS processes are being updated, maintained, and practiced;
3) Data showing that the SRM process has been conducted on all Element 2.1 (1) Hazard Identification and Analysis items;
4) Data showing compliance with Process 2.1.1 System Description and Analysis;
5) Data showing compliance with Element 3.2 Management of Change;
6) Data showing compliance with Element 4.1 Competencies and Training;
7) All applicable SMS processes and procedures have been applied to at least one existing hazard and the mitigation process has been initiated;
8) Complete SMS training for the staff directly involved in the SMS process to the level of accomplishing all SMS processes; and
9) Complete employee training commensurate with this level of implementation phase maturity.

Documents

All processes and procedures for operating the SMS should be documented. This document, or documents, should cover all processes and procedures necessary from information gathering through SRM and mitigation. As the SA processes are not mature enough, at this point, to be verifiable, as a minimum the policy and procedures will be documented. The organization must provide documentation for the following:

1) Data showing that SRM processes and procedures have been applied to all Element 2.1 (1) Hazard Identification and Analysis items;
2) Data showing that SRM processes and procedures have been applied to at least one existing hazard and that the mitigation process has been initiated;
3) Updated SMS implementation plan for all elements; and
4) Updated SMS Training Plan for all employees participating within the scope of the pilot project).

When conducting the document review and assessment, the objective is to develop and implement the specific processes and procedures necessary for applying SMS proactively for the systems listed in the *SMS Framework*, Element 1.1 (3), as appropriate.

At completion of Level 3, the PMT and the POC will begin the SMS Pilot Project and Voluntary Program Validation (Section 11.1– SMS Participant Assessment Process) and ensure a Letter of Participation (Attachment 5 – Example Letter of Acknowledgement) is delivered to the organization.

The Level 3 Exit Criteria Worksheet is Attachment 3 – Level 3 Exit Criteria Worksheet. This worksheet is used by the PMT to establish when a participant can proceed to the next level within the pilot project. The worksheet includes the outputs and output documents listed above. The exit criteria worksheet is not intended to hold a participant from implementing any part of their SMS system at any time. The worksheet aids the PMT and the participant to progress from one level of maturity to the next and standardizes the implementation of an SMS during pilot project development.

Level 4 – Detailed Guidance and Expectations

Level 4: Continuous Improvement

The final level of SMS maturity is the continuous improvement level. Processes have been in place and their performance and effectiveness has been verified. The complete SA process, including continuous monitoring and the remaining features of the other SRM and SA processes are functioning. A major objective of a successful SMS is to attain and maintain this continuous improvement status for the life of the organization.

Level 4 Objective

The overall objective of SMS development is captured in the first objective of the policy component of the *SMS Framework*:

"The Service Provider will develop and implement an integrated, comprehensive SMS for its entire organization."

The specific objective of Level 4 is for the organization to verify the performance and effectiveness of their SMS management practices and operational processes.

Attachment 1 – Level 1 Exit Criteria Worksheet

Exit - Level 1 Criteria - Worksheet			
To be completed during Level 1 Validation Session. Forward completed copy to SMS PMTL.			
Exit Criteria	**Validated**	**Initials**	**Date**
1. Data showing of top management's commitment to implement SMS, define safety policy, and convey safety expectations and objectives to its employees (***SMS Framework*** Element 1.1; "Safety Policy")			
2. Data showing adequate resources are available to implement SMS (in accordance with ***SMS Framework*** Sub-Element 1.2(2) Management Commitment and Safety Accountabilities			
3, Designation of a management representative who will be responsible for SMS development (***SMS Framework*** Sub-Element 1.3 (1))"Key Safety Personnel"			
4. Obtain agreement with FAA on Detailed Gap Analysis for the entire organization* on all elements of the ***SMS Framework*** **Entire organization participating within the scope of the system description.* (Reference ***Design & Manufacturing SMS Pilot Project Guide***, Section 5, 8 & 9)			
5. Obtain agreement with FAA on an SMS Implementation Plan addressing implementation of all gaps of the ***SMS Framework*** to take the entire organization* through Level 4) **Entire organization participating within the scope of the system description. (* *Reference*(APPENDIX C: Tools and Templates)			
6. Identified safety competencies necessary in accordance with *SMS Framework* Sub-Element 4.1.1 Personnel Expectations (Competence) item (1). and; Complete training commensurate with Level 1 implementation phase of maturity for those competencies, and develop a training program for all employees participation within the scope of the system description (in accordance with *SMS Framework* Sub-Element 4.1.2 Training). **All employees participating in the system description*			
Output Documents	**Document Attached?**		
1. Safety Policy	☐ Yes ☐ No		
2. Detailed Gap Analysis	☐ Yes ☐ No		
3. Comprehensive SMS implementation plan (Summary) for the entire* organization through SMS Implementation Level 4 (within the scope of the system description	☐ Yes ☐ No		

4. SMS Training Plan for all employees (employees participating within the scope of the system description).	☐ Yes ☐ No

The undersigned attest to the participation of _____ in the FAA SMS Pilot Project (SMS PP) and their associated accomplishment in the development, through Level 1, of their SMS.

PMTL:

PPL or MSMS Lead:

Attachment 2 – Level 2 Exit Criteria Worksheet

Exit - Level 2 Criteria - Worksheet

To be completed during Level 2 joint assessment. Forward completed copy to SMS PMTL.

Exit Criteria	Validated	Initials	Date
1. Documented processes and procedures for operating the SMS to the level of reactive analysis, assessment, and mitigating actions			
2. Develop documentation relevant to SMS implementation plan and SRM components (reactive processes)			
3. Initiated and document voluntary non-punitive employee reporting and feedback program			
4. Completed SMS training for the staff directly involved in the SMS process to at least the level necessary for the SMS reactive processes			
5. Apply SRM processes and procedures to at least one known (existing) hazard and initiate the mitigation process to control/mitigate the risk associated with the hazard			
6. Updated detailed gap analysis on the entire* organization for all elements of the ***SMS Framework (witin the scope of the system description)***			
7. Update comprehensive SMS implementation plan for all elements to take the organization through Level 4 (within the scope of the system description)			

Output Documents	Document Attached?
1. Data showing that SRM processes and procedures have been applied to at least one existing hazard and that the mitigation process has been initiated	☐ Yes ☐ No
2. Updated comprehensive SMS implementation plan (or summary) for all elements to take the organization through Level 4	☐ Yes ☐ No
3. Updated SMS Training Plan for all employees participating in the pilot project	☐ Yes ☐ No

The undersigned attest to the participation of _____ in the FAA SMS Pilot Project (SMS PP) and their associated accomplishment in the development, through Level 2, of their SMS.

PMTL:

PPL or MSMS Lead:

Attachment 3 – Level 3 Exit Criteria Worksheet

Exit - Level 3 Criteria - Worksheet			
To be completed during Level 3 Validation Session. Forward completed copy to SMS PMTL.			
Exit Criteria	**Validated**	**Initials**	**Date**
1. Demonstrated performance of Level 2 Expectations			
2. Data showing that all SMS processes are being updated, maintained, and practiced			
3. Data showing that the SRM process has been conducted on all Element 2.1 (1) Hazard Identification and Analysis items			
4. Data showing compliance with Process 2.1.1 System Description & Analysis			
5. Data showing compliance with Element 3.2 Management of Change			
6. Data showing compliance with Element 4.1 Competencies & Training;			
7. All applicable SMS processes and procedures have been applied to at least one existing hazard and the mitigation process(s) has been initiated			
8. Complete SMS training for the staff directly involved in the SMS process to the level of accomplishing SMS processes			
9. Complete employee training commensurate with this level of implementation maturity.			
Output Documents	**Document Attached?**		
1. Data showing that SRM processes and procedures have been applied to all Element 2.1 (1) Hazard Identification and Analysis items	☐ Yes ☐ No		
2. Data showing that all SRM processes and procedures have been applied to at least one existing hazard and that the mitigation process has been initiated	☐ Yes ☐ No		
3. Updated comprehensive SMS implementation plan (or summary) for all SMS elements (within the scope of the system description)	☐ Yes ☐ No		
4. Updated SMS Training Plan for all employees participating in the pilot project	☐ Yes ☐ No		
The undersigned attest to the participation of _____in the FAA SMS Pilot Project (SMS PP) and their associated accomplishment in the development, through Level 3, of their SMS implementation.			

PMTL:
PPL or MSMS Lead:

Attachment 4 – Sample Onsite Implementation Assessment Notification

Dear Mr./ Ms. _____

The Federal Aviation Administration (FAA) thanks you for your voluntary participation in the FAA's Design and Manufacturing (D&M) Safety Management System (SMS) Pilot Project.

Based on our review of your company's submitted documents, we have determined that your SMS processes meet the expectations of the Aircraft Certification Service's (AIR) SMS Framework and the D&M SMS Pilot Project Guide for the processes submitted.

FAA acknowledgement of your completion of SMS Level X is contingent upon the FAA's onsite implementation assessment of your organization's facilities, operations, and records to verify that your company has met Level X SMS expectations. Please note that a successful assessment of your company's achievements does not imply formal FAA acceptance or approval of your SMS or its components, but does recognize your participation in this vital phase of SMS development.

Therefore, we would like to schedule an onsite assessment of your organization's SMS between (start date) to (end date) at a mutually agreeable time. The assessment will encompass SMS elements (x.x, y.y…). The assessment process will include the following facilities/functions: ….

The (FAA PMT Lead designated / principal assessor) for this assessment is (Mr./Ms.) (name) who may be reached at (telephone number or email). (His/Her) address is (office address).

The FAA requests the attendance by a Senior Management representative from each facility to be evaluated as well as cognizant technical and supervisory personnel during the pre-assessment and post- assessment conferences. To ensure that the assessment is conducted smoothly and with minimal disruption to your staff, the FAA further recommends that you provide escorts who are knowledgeable in the various areas to be reviewed.

If you have any questions concerning the scheduling of this assessment, please feel free to contact me. Questions or comments concerning its conduct should be sent to the PMT Lead/principal assessor.

We are grateful for your participation in this pilot project and its contribution to the continuous improvement in aviation safety.

/s/

FAA D&M SMS Pilot Project Lead

Attachment 5 – Example Letter of Acknowledgement

Letter of Acknowledgement

Safety Management System Pilot Project

Participation: Level [One, Two or Three]

Dear Mr./Ms. _____

This is to acknowledge the participation of [company's name] in the Federal Aviation Administration's (FAA) Safety Management System (SMS) pilot project. Based on our review of your company's plans, documentation, and activities, we have determined that your SMS project meets the expectations of the Aircraft Certification Service's (AIR) Manufactures *SMS Framework* for [Level One, Level 2 SMS, Level 3 SMS.]. This achievement has been validated by representatives of your FAA Participant Management Team.

The FAA currently does not have regulatory requirements for SMS but is considering SMS regulations. The AIR SMS Pilot Projects consists of voluntary SMS implementation by design and production providers. The *MSMS Framework* used in the project is based upon the requirements of Order VS 8000.367, Appendix B, Annex 8 of the International Civil Aviation Organization (ICAO) document No. 9859 *Safety Management Manual and the 14 CFR Part 5 FAA Notice of Proposed Rulemaking*.

This assessment of your company's achievements does not imply formal FAA acceptance or approval of your SMS or its components but does recognize your active participation in this vital phase of development.

We are grateful for your participation in this pilot project and its contribution to continuous improvement in aviation safety.

/s/

Aircraft Certification Service

APPENDIX C: Tools and Templates

This appendix includes screenshots for each of tab of the Gap Analysis Tool (GAT) spreadsheet. The Gap tool is available on SharePoint or can be provided by the PMTL.

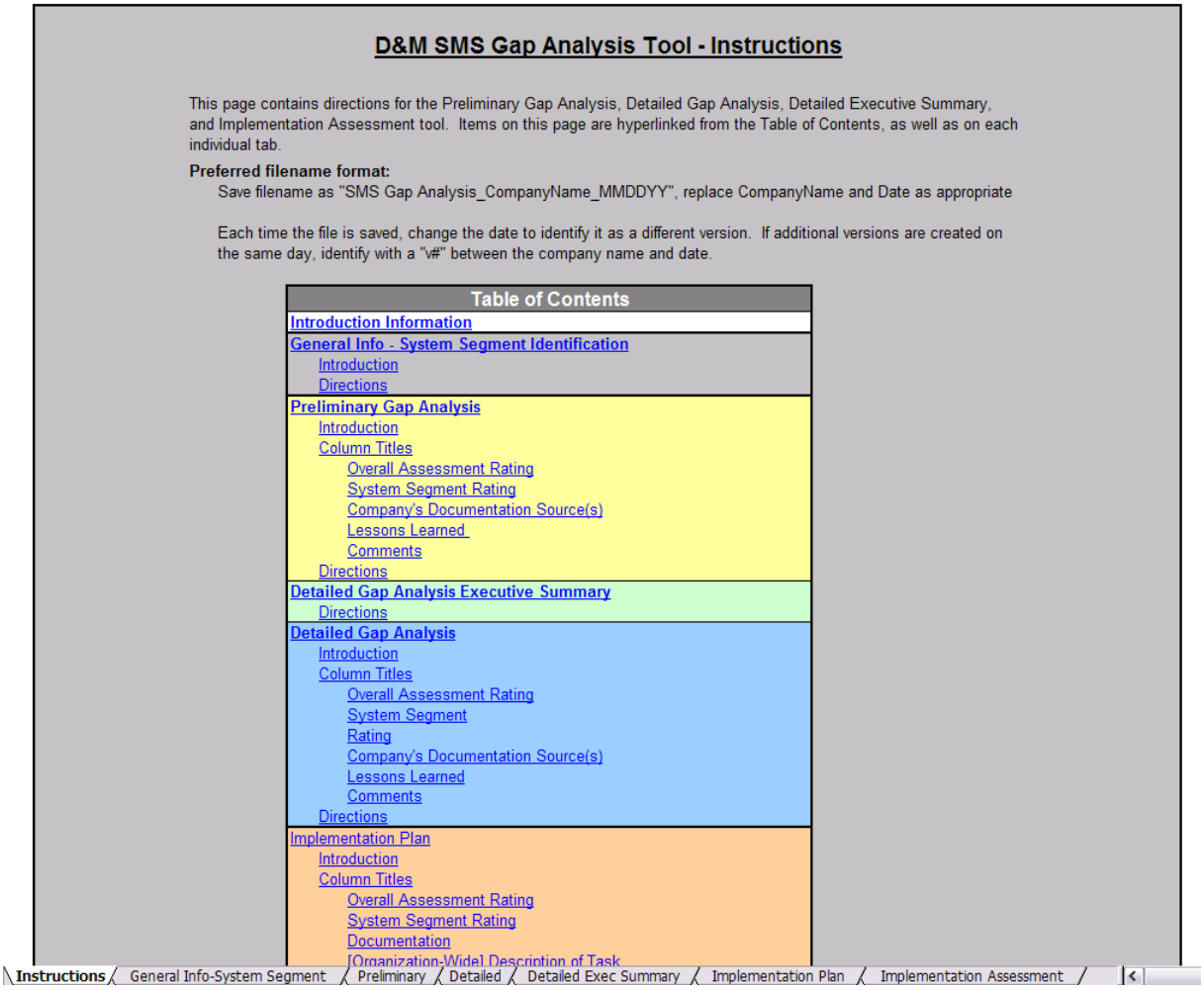


Figure 6 – View of Gap Analysis Tool (Instructions Tab)

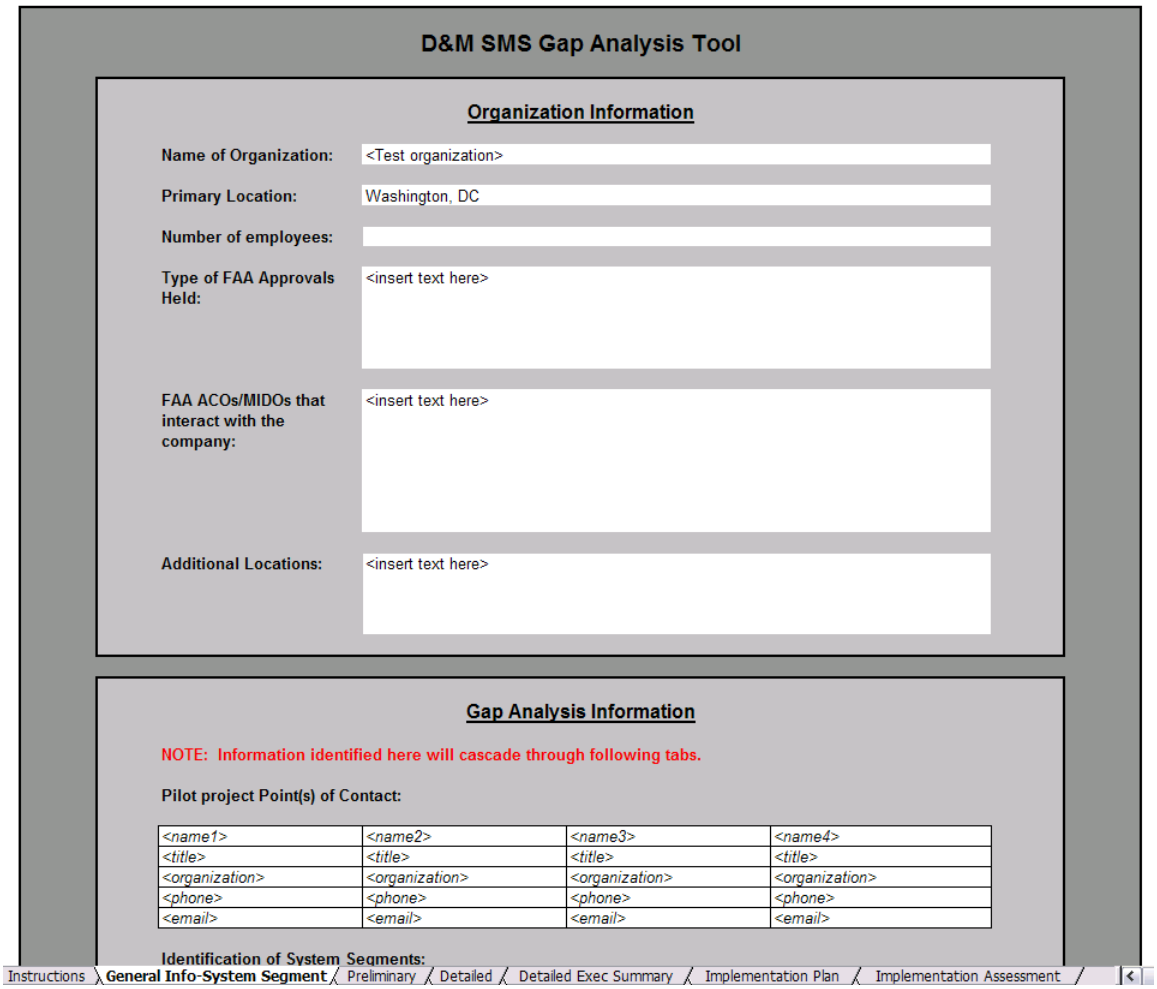


Figure 7 – View of Gap Analysis Tool (General Info Tab)

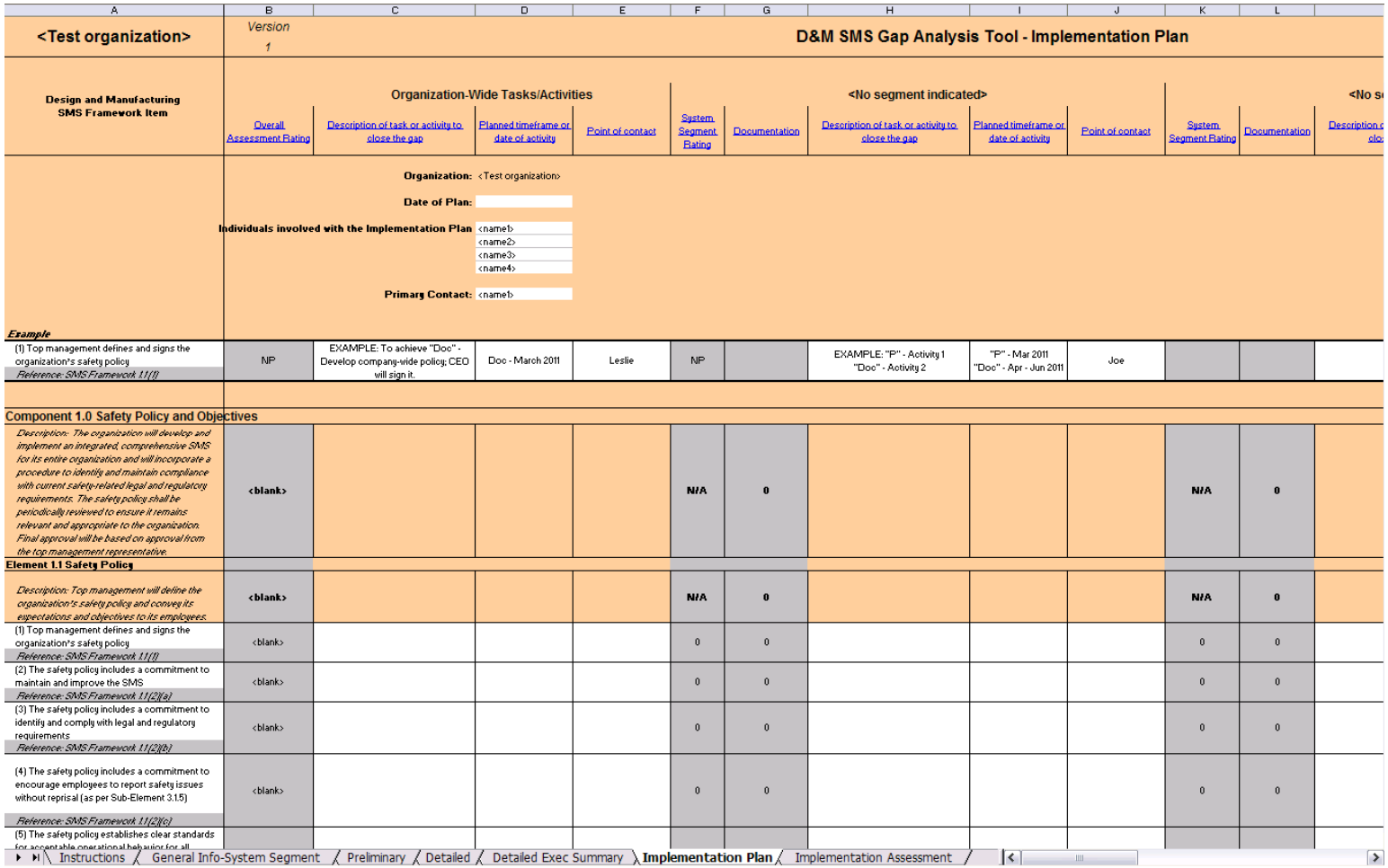
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
<Test organization>	*Version 1*	**D&M SMS Gap Analysis Tool - Preliminary Assessment**												
Design and Manufacturing SMS Framework Item	**Overall Assessment Rating**	**System Segments Rating** <No segment indicated>	<No segment indicated>	<No segment indicated>	<No segment indicated>	<No segment indicated>	<No segment indicated>	<No segment indicated>	<No segment indicated>	<No segment indicated>	<No segment indicated>	**Organization's Documentation Source(s)** *[optional]*	**Lessons Learned**	**Comments**
	Organization: <Test organization>													
	Date of Assessment:													
	Individuals involved with the assessment:	<name1>												
		<name2>												
		<name3>												
		<name4>												
	Primary Contact:	<name2>												
Component 1.0 Safety Policy and Objectives														
The organization developed and implements an integrated, comprehensive SMS for its entire organization and will incorporate a procedure to identify and maintain compliance with current safety-related legal and regulatory requirements. The safety policy is periodically reviewed to ensure it remains relevant and appropriate to the organization. Final approval is based on approval from the top management representative.	**<blank>**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**			
Element 1.1 Safety Policy														
Top management defines the organization's safety policy and convey its expectations and objectives to its employees	**<blank>**													
Element 1.2 Management Commitment and Safety Accountabilities														
Management defines, documents, and communicates the safety roles, responsibilities, and authorities throughout its organization.	**<blank>**													
Element 1.3 Designation and Responsibilities of Required Safety Management Personnel.														
Designation and responsibilities of required safety management personnel.	**<blank>**													
Element 1.4 Emergency Preparedness and Response														
The organization developed and implements procedures, as necessary, that it will follow in the event of an accident or incident.	**<blank>**													
Element 1.5 SMS Document and Records														
The organization has documented safety policies, objectives, procedures, a document/record management process and a safety management plan that meet organizational safety requirements and objectives.	**<blank>**													
Component 2.0 Safety Risk Management (SRM)														
The organization has developed processes to determine the critical characteristics of its systems and operational environment and apply this knowledge to identify hazards, analyze and	**<blank>**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**			

Instructions | General Info-System Segment | **Preliminary** | Detailed | Detailed Exec Summary | Implementation Plan | Implementation Assessment

Figure 8 – View of Preliminary Gap Analysis Tool

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
<Test organization>	Version 1	D&M SMS Gap Analysis Tool - Detailed Assessment																				
Design and Manufacturing SMS Framework Item	Overall Assessment Rating	System Segments: <No segment indicated> Rating	Doc Source	<No segment indicated> Rating	Doc Source	<No segment indicated> Rating	Doc Source	<No segment indicated> Rating	Doc Source	<No segment indicated> Rating	Doc Source	<No segment indicated> Rating	Doc Source	<No segment indicated> Rating	Doc Source	<No segment indicated> Rating	Doc Source	<No segment indicated> Rating	Doc Source	<No segment indicated> Rating	Doc Source	Lessons Learned
	Organization: <Test organization>																					
	Date of Assessment:																					
	Individuals involved with the assessment: <name1> <name2> <name3> <name4>																					
	Primary Contact: <name1>																					
Component 1.0 Safety Policy and Objectives																						
Description: The organization will develop and implement an integrated, comprehensive SMS for its entire organization and will incorporate a procedure to identify and maintain compliance with current safety-related legal and regulatory requirements. The safety policy shall be periodically reviewed to ensure it remains relevant and appropriate to the organization. Final approval will be based on approval from the top management representative.	<blank>	N/A		N/A		N/A		N/A		N/A		N/A		N/A		N/A		N/A		N/A		
Element 1.1 Safety Policy																						
Description: Top management will define the organization's safety policy and convey its expectations and objectives to its employees.	<blank>	N/A		N/A		N/A		N/A		N/A		N/A		N/A		N/A		N/A		N/A		
(1) Top management defines and signs the organization's safety policy *Reference: SMS Framework 1.1(1)*	<blank>																					
(2) The safety policy includes a commitment to maintain and improve the SMS *Reference: SMS Framework 1.1(2)(a)*	<blank>																					
(3) The safety policy includes a commitment to identify and comply with legal and regulatory requirements *Reference: SMS Framework 1.1(2)(b)*	<blank>																					
(4) The safety policy includes a commitment to encourage employees to report safety issues without reprisal (as per Sub-Element 3.1.5) *Reference: SMS Framework 1.1(2)(c)*	<blank>																					
(5) The safety policy establishes clear standards for acceptable operational behavior for all employees *Reference: SMS Framework 1.1(2)(d)*	<blank>																					
(6) The safety policy provides management guidance for setting safety objectives *Reference: SMS Framework 1.1(2)(e)*	<blank>																					
(7) The safety policy provides management																						

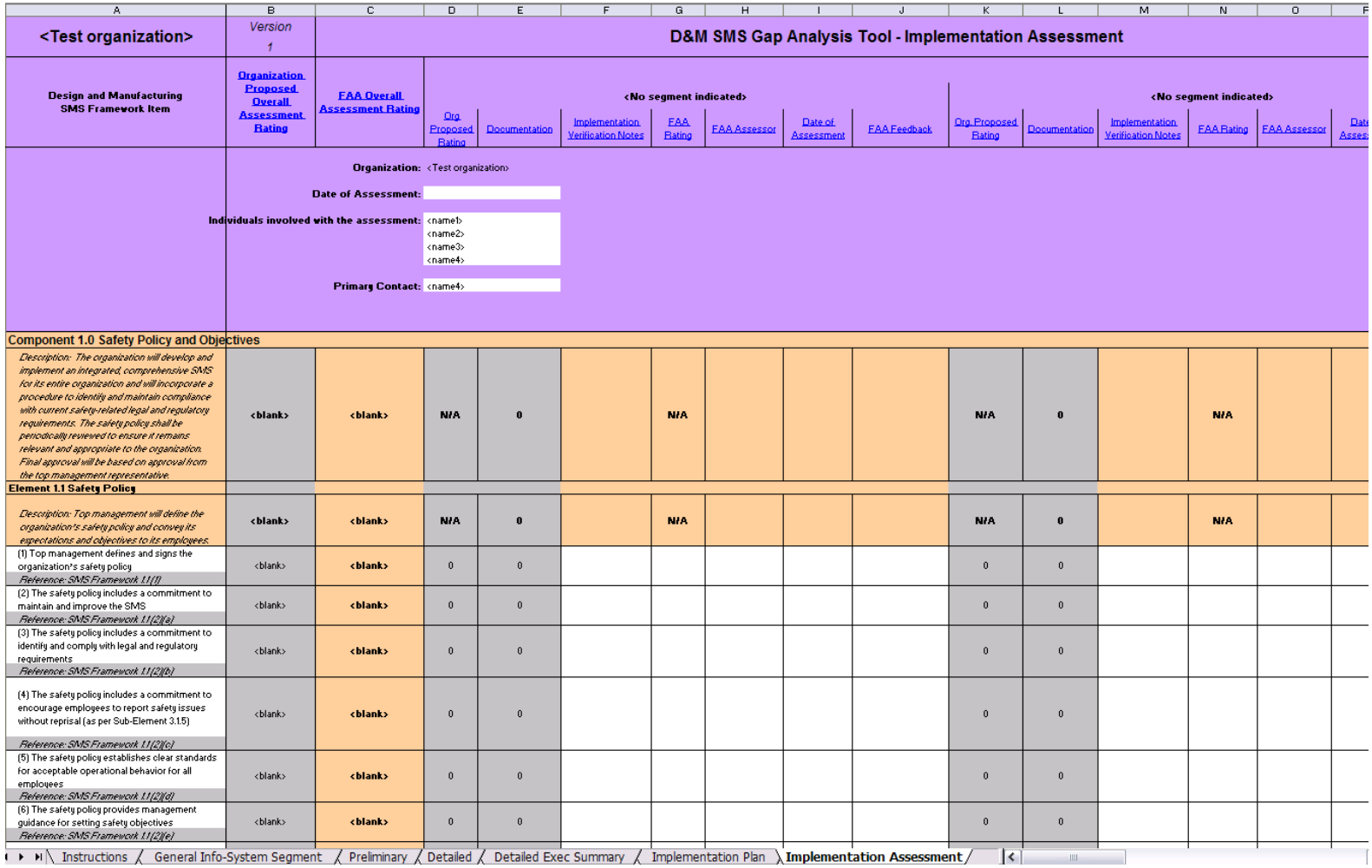
Figure 9 – View of Detailed Gap Analysis Tool



A	B	C	D	E	F	G	H	I	J	K	L	
<Test organization>	*Version 1*	**D&M SMS Gap Analysis Tool - Implementation Plan**										
Design and Manufacturing SMS Framework Item		Organization-Wide Tasks/Activities					<No segment indicated>					<No s
	Overall Assessment Rating	Description of task or activity to close the gap	Planned timeframe or date of activity	Point of contact	System Segment Rating	Documentation	Description of task or activity to close the gap	Planned timeframe or date of activity	Point of contact	System Segment Rating	Documentation	Description clos
		Organization: <Test organization>										
		Date of Plan:										
		Individuals involved with the Implementation Plan	<name1>									
			<name2>									
			<name3>									
			<name4>									
		Primary Contact:	<name1>									
Example												
(1) Top management defines and signs the organization*'s* safety policy *Reference: SMS Framework 1.1 (1)*	NP	EXAMPLE: To achieve "Doc" - Develop company-wide policy; CEO will sign it.	Doc - March 2011	Leslie	NP		EXAMPLE: "P" - Activity 1 "Doc" - Activity 2	"P" - Mar 2011 "Doc" - Apr - Jun 2011	Joe			
Component 1.0 Safety Policy and Objectives												
Description: The organization will develop and implement an integrated, comprehensive SMS for its entire organization and will incorporate a procedure to identify and maintain compliance with current safety-related legal and regulatory requirements. The safety policy shall be periodically reviewed to ensure it remains relevant and appropriate to the organization. Final approval will be based on approval from the top management representative.	**<blank>**				**N/A**	**0**				**N/A**	**0**	
Element 1.1 Safety Policy												
Description: Top management will define the organization's safety policy and convey its expectations and objectives to its employees.	**<blank>**				**N/A**	**0**				**N/A**	**0**	
(1) Top management defines and signs the organization*'s* safety policy *Reference: SMS Framework 1.1 (1)*	<blank>				0	0				0	0	
(2) The safety policy includes a commitment to maintain and improve the SMS *Reference: SMS Framework 1.1 (2)(a)*	<blank>				0	0				0	0	
(3) The safety policy includes a commitment to identify and comply with legal and regulatory requirements *Reference: SMS Framework 1.1 (2)(b)*	<blank>				0	0				0	0	
(4) The safety policy includes a commitment to encourage employees to report safety issues without reprisal (as per Sub-Element 3.1.5) *Reference: SMS Framework 1.1 (2)(c)*	<blank>				0	0				0	0	
(5) The safety policy establishes clear standards for acceptable operational behavior for all												

Instructions | General Info-System Segment | Preliminary | Detailed | Detailed Exec Summary | **Implementation Plan** | Implementation Assessment

Figure 10 – View of Implementation Plan Tab



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
<Test organization>	*Version 1*	**D&M SMS Gap Analysis Tool - Implementation Assessment**													
Design and Manufacturing SMS Framework Item	**Organization Proposed Overall Assessment Rating**	**FAA Overall Assessment Rating**	**<No segment indicated>** Org. Proposed Rating	Documentation	Implementation Verification Notes	FAA Rating	FAA Assessor	Date of Assessment	FAA Feedback	**<No segment indicated>** Org. Proposed Rating	Documentation	Implementation Verification Notes	FAA Rating	FAA Assessor	Date Assess
		Organization: <Test organization>													
		Date of Assessment:													
		Individuals involved with the assessment:	<name1> <name2> <name3> <name4>												
		Primary Contact:	<name4>												
Component 1.0 Safety Policy and Objectives															
Description: The organization will develop and implement an integrated, comprehensive SMS for its entire organization and will incorporate a procedure to identify and maintain compliance with current safety-related legal and regulatory requirements. The safety policy shall be periodically reviewed to ensure it remains relevant and appropriate to the organization. Final approval will be based on approval from the top management representative.	**<blank>**	**<blank>**	**N/A**	**0**		**N/A**				**N/A**	**0**		**N/A**		
Element 1.1 Safety Policy															
Description: Top management will define the organization's safety policy and convey its expectations and objectives to its employees.	**<blank>**	**<blank>**	**N/A**	**0**		**N/A**				**N/A**	**0**		**N/A**		
(1) Top management defines and signs the organization's safety policy *Reference: SMS Framework 1.1(1)*	<blank>	**<blank>**	0	0						0	0				
(2) The safety policy includes a commitment to maintain and improve the SMS *Reference: SMS Framework 1.1(2)(a)*	<blank>	**<blank>**	0	0						0	0				
(3) The safety policy includes a commitment to identify and comply with legal and regulatory requirements *Reference: SMS Framework 1.1(2)(b)*	<blank>	**<blank>**	0	0						0	0				
(4) The safety policy includes a commitment to encourage employees to report safety issues without reprisal (as per Sub-Element 3.1.5) *Reference: SMS Framework 1.1(2)(c)*	<blank>	**<blank>**	0	0						0	0				
(5) The safety policy establishes clear standards for acceptable operational behavior for all employees *Reference: SMS Framework 1.1(2)(d)*	<blank>	**<blank>**	0	0						0	0				
(6) The safety policy provides management guidance for setting safety objectives *Reference: SMS Framework 1.1(2)(e)*	<blank>	**<blank>**	0	0						0	0				

Instructions | General Info-System Segment | Preliminary | Detailed | Detailed Exec Summary | Implementation Plan | **Implementation Assessment**

Figure 11 – View of Assessment Tool

APPENDIX D: System Description & Hazard Identification Process

System Description and Analysis Summary

Prior to performing the preliminary gap analysis process, the PMT will assist the company in conducting a System Description and Analysis of the company's operational functions.

1) Every system contains inherent potential safety vulnerabilities which are characterized in terms of hazards. The boundaries of the system, as per its formal description, must therefore be sufficiently wide to encompass all possible hazards that the system could confront or generate. The system description should consider three aspects of the system: product, process, and organization.

2) The safety consequences of a potential loss or degradation of the system will be determined, in part, by the characteristics of the operational environment in which the system will be operated. The description of the environment should therefore include any factors that could have a significant effect on safety. These factors will vary from one organization to another. They could include, for example, geographic operational locations, owned vs. leased equipment and facilities, contractor relationships and/or union representation.

The appendix below is intended to provide an organization with one possible alternative for creating a system description that can facilitate hazard identification. It is not mandatory and does not constitute regulation but is included in this guide as a way that an organization can approach SMS.

System Description and Hazard Identification: A Process for Design and Manufacturing Organizations

Alan J. Stolzer, Ph.D.

Embry-Riddle Aeronautical University

PURPOSE

a) This appendix:

i) Presents a procedure for a Design and/or Manufacturer (D&M) firm to follow in order to create a system description of its organization.

ii) Should be used after and in concert with the D&M Safety Management System (SMS) Pilot Project Guide, which fully explains SMS for D&M firms.

iii) Shows how the system description plays a key part in a company's SMS, supporting other efforts such as safety policy, risk management, safety assurance, and safety promotion.

iv) Explains that, while an organization may employ existing management systems and/or other hazard and risk tools[6], the intent of a system description is, in part, to identify the existence and placement of these analysis methods within the organization or the absence thereof.

b) This appendix is not mandatory and does not constitute regulation. There are a variety of ways that an organization can approach SMS. This appendix is intended to provide an organization with one possible alternative for creating a system description that can facilitate hazard identification.

APPLICABILITY

This appendix applies to companies that design and/or manufacture products for aviation, from large systems such as airliners, to smaller systems such as engines and propellers, to supporting parts such as batteries, starters, and fittings. While the text refers to D&M companies, this is done for brevity. Whenever D&M is referred to, the reader should understand "design and/or manufacturer."

For those instances where crossover designs exist (i.e., where one organization designs and another manufactures), the procedure will guide the user through such identification. The term D&M is meant to include this type of arrangement.

RELATED READING MATERIAL

The following references, current editions, may be of value to users of this appendix, as they develop their system descriptions:

- International Civil Aviation Organization (ICAO) Document 9859, ICAO Safety Management Manual (SMM, Second Edition, 2009)
- Advisory Circular (AC) 120-92A, Safety Management Systems for Aviation Service Providers[7]
- FAA Order 8000.369, Safety Management System Guidance.

[6] For example, Failure Modes and Effects Analysis (FMEA) or Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis.

[7] Although this Advisory Circular was created for operators and maintenance service providers, the fundamental SMS principles are relevant to D&M.

- FAA Order VS 8000.367, Aviation Safety (AVS) Safety Management System Requirements

Hazard Identification References.

- Bahr, N. J. (1997). *System safety engineering and risk assessment: A practical approach.* New York: Taylor & Francis.

- Ericson, C. A. (2005). *Hazard analysis techniques for system safety*. Hoboken, NJ: John Wiley & Sons.

- Manuele, F. A. (2003). *On the practice of safety, 3rd edn*. Hoboken, NJ: John Wiley & Sons.

- Mikulak, R. J., McDermott, R., Beauregard, M. (2008). *The basics of FMEA, 2nd edn.* Unknown: Productivity Press.

- Petersen, D. (2003). *Techniques of safety management: A systems approach, 4th edn.* Des Plaines, IL: American Society of Engineers.

- Roland, H. E., & Moriarty, B. (1990). *System safety engineering and management, 2nd edn.* Hoboken, NJ: John Wiley & Sons.

- Stephenson, J. (1991). System safety 2000: A practical guide for planning, managing, and conducting systems safety programs. Hoboken, NJ: John Wiley & Sons.

- Stolzer, A. J., Halford, C. D., & Goglia, J. J. (2008). *Safety management systems in aviation*. Burlington, VT: Ashgate Publishing.

BACKGROUND

The user of this procedure should be familiar with the role that SMS will play in all aviation enterprises. The recommended reading material, particularly the ICAO and FAA documents, provides this background.

a) A system description can be thought of as an account of organizational structures, procedures, processes, people, equipment, and facilities used to accomplish the organization's mission.

   i) The process used to identify hazards must consider all components of the system design; thus, it is necessary to begin with a system description that takes into account those components and their interactions.

   ii) While individual parts or functions of the organization may have descriptions and hazard elements, the intent of this description is to bring together those elements into an overarching view of the system as a whole; thereby enabling overall system analysis.

   iii) There is no specified format for a system description, but it should be thoroughly and effectively documented.

b) D&M companies differ from other aviation industry businesses in that they:

i) Must deal with product lifecycles, such as requirements, design, testing and certification, production, support, and product retirement.

ii) Have to manage the safety of their fielded product, as well as the processes that create the product.

iii) Generally have a quality management system in place, such as AS9100[8], that may simplify the development of a system description, the identification of hazards, and the implementation of SMS.

c) A system description provides a detailed view of an organization sufficient to relate hazards to parts of the description. The system description provides the foundation upon which proactive hazard identification can occur.

d) The procedure defined in this document is intended to guide an organization through the process of creating a system description to facilitate proactive hazard identification. The focus of the present procedure is on the development of a system description. The user should refer to other resources for specific techniques regarding hazard identification.

e) The desired outcomes of this procedure are:

i) To develop an organization's understanding of a system description;

ii) To create a system description for your organization; and

iii) To develop an initial set of high-level hazards for further analysis.

f) The desired outcomes of this procedure are:

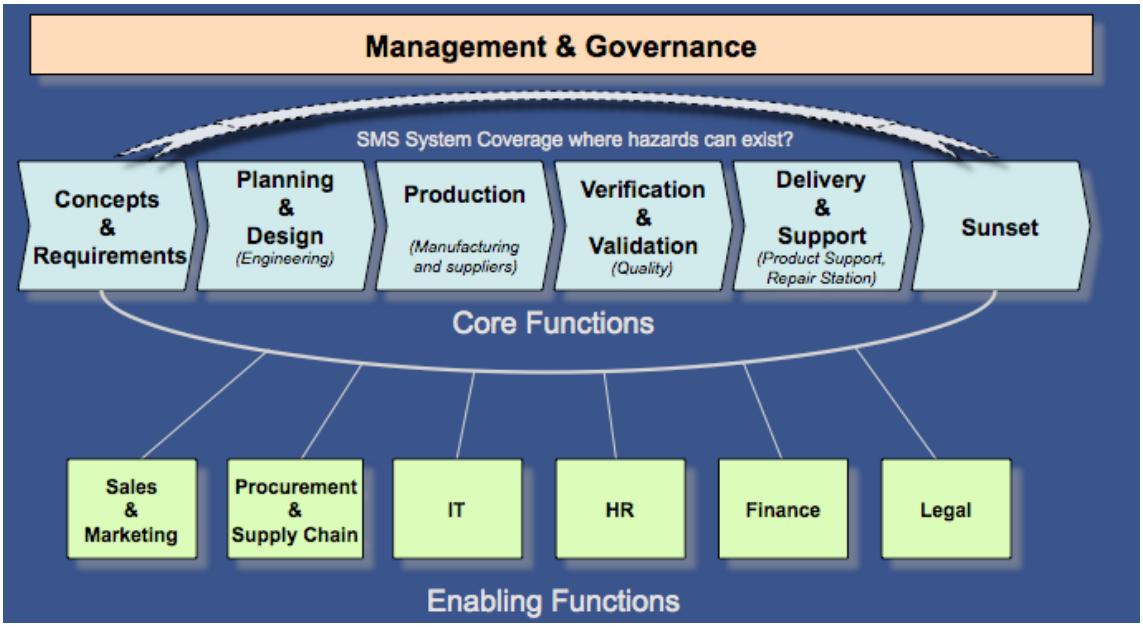
i) To develop an organization's understanding of a system description.

ii) To create a system description for your organization; and

iii) To develop an initial set of high level hazards for further analysis.

[8] AS9100 is a family of standards contains all of the requirements of ISO 9001:2008, the global standard for quality management systems, in addition to numerous additional requirements specific to the aerospace industry.

FIGURE 1. DESIGN & MANUFACTURING VALUE CHAIN



PROCEDURE OVERVIEW

The system description procedure consists of the steps shown in Figure 1. Each step of the procedure is expanded on in this appendix.

a) The procedure is most effective when carried out in a group environment. The core constituents of the group should be upper management, which controls the organization's resources and draws upon other staff members to develop the system description details defined by each step.

b) The system description procedure will touch on many aspects of an organization's operations and, as such, may generate large amounts of information. The suggested format to collect the information is to use wallboards to post notes of information discovered in each step, or electronic aids such as mind mapping software. The system description effort will require a significant amount of time to assemble and compile the raw data, and involve a number of individuals. While certain departments of the organization may be excluded from the process, such exclusions must be done deliberately and with caution. The intent of a system description is to include all facets of an organization, at the appropriate level. For example, while janitorial may be excluded from the system description, what if janitorial at night can disrupt calibration of manufacturing equipment? Consider the ramification of such exclusions.

c) Throughout this procedure, the user should remain cognizant of the end goal, which is to identify hazards that may exist in the organization. Although it is advisable not to focus excessively on hazard identification during the development of the system description, the user may find that some hazards become apparent; these should be recorded. A hazard numbering scheme should be developed and used throughout the procedure.

d) Upper management must create an environment for success. Sufficient time must be allocated to procedure execution. To preclude the rank and file perceiving this as unimportant, it is vital that managements set expectations regarding the procedure, including strategies to avoid fatigue and

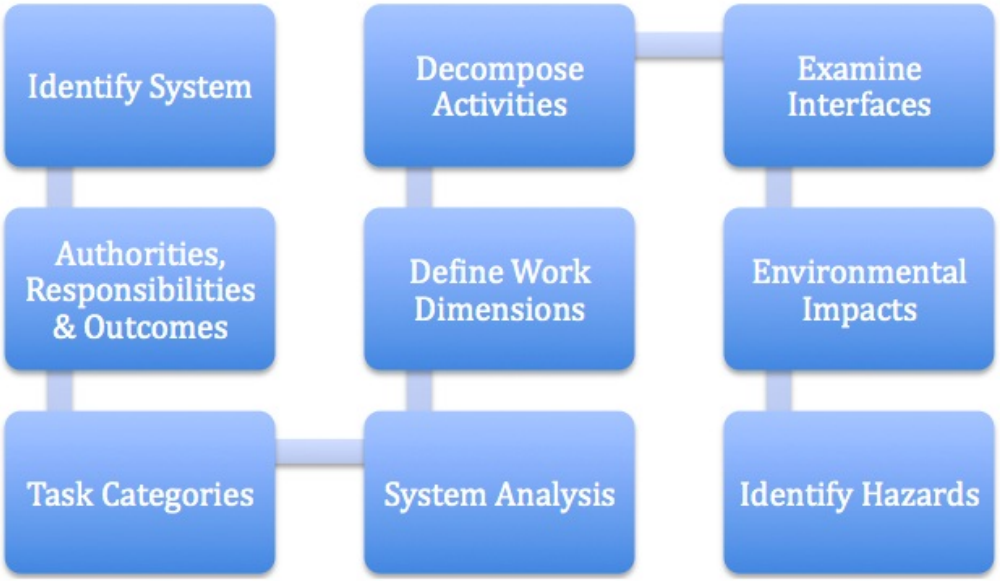
conflict during its execution.

e) Most steps of the procedure will ask the organization to examine itself from the perspective of *product lifecycle* as well as different *domains* of an organization:

i) The *product lifecycle* refers to stages of product, such as requirements, design, testing, certification, production, delivery, support, and retirement.

ii) The *domain* is less obvious but equally important in discovering details at each step in the process. Domains refer to *Organization*, *Design*, *Process*, and *Product.* Generally, the *organizational* domain consists of such areas as accounting, human resources, marketing departments, etc. The *Design* domain refers to the methods an organization uses to execute its designs. The *Process* domain refers to the methods an organization uses to make its products such as material selection, tooling, shop procedures, etc. The *Product* domain is the product you sell. For design-only houses where no parts manufacture or assembly occurs, this "product" is usually an FAA-approved design.

FIGURE 1. SYSTEM DESCRIPTION PROCEDURE OVERVIEW



PROCEDURE

a) **IDENTIFY SYSTEM**

This step consists of broadly identifying what your organization does. Figure 2 shows a graphical way to identify a system in terms of the inputs to the organization, the outputs - what is produced, the resources required, the controls guiding the processes, and in the center, the activities that make up the organization. Subsequent steps in the procedure expand upon this first step.

Responding to the following points, organized by *domain*, will aid the user with this step. *Note*: these

are samples of questions that may be asked. Some will not be relevant for every organization; simply disregard. Add other questions/issues as appropriate.

i) *Organizational Domain*

- What is the type of organization – Design? Manufacturer? Both?
- Describe the resources used by the organization. How many employees? What type of employee skills? Who are the customers? What facilities does the organization use? Who are the suppliers? What information systems are used in the organization?
- What reputation does the organization hold in its product sector? How important is reputation? Is there a reputable product base?

ii) *Design Domain*

- What methods are used to identify hazards?
- Describe existing design methods.
- What are the regulatory constraints?
- How is design documentation control performed?
- How is organization knowledge maintained over time, i.e., artifacts of prior designs or methods?

iii) *Process Domain*

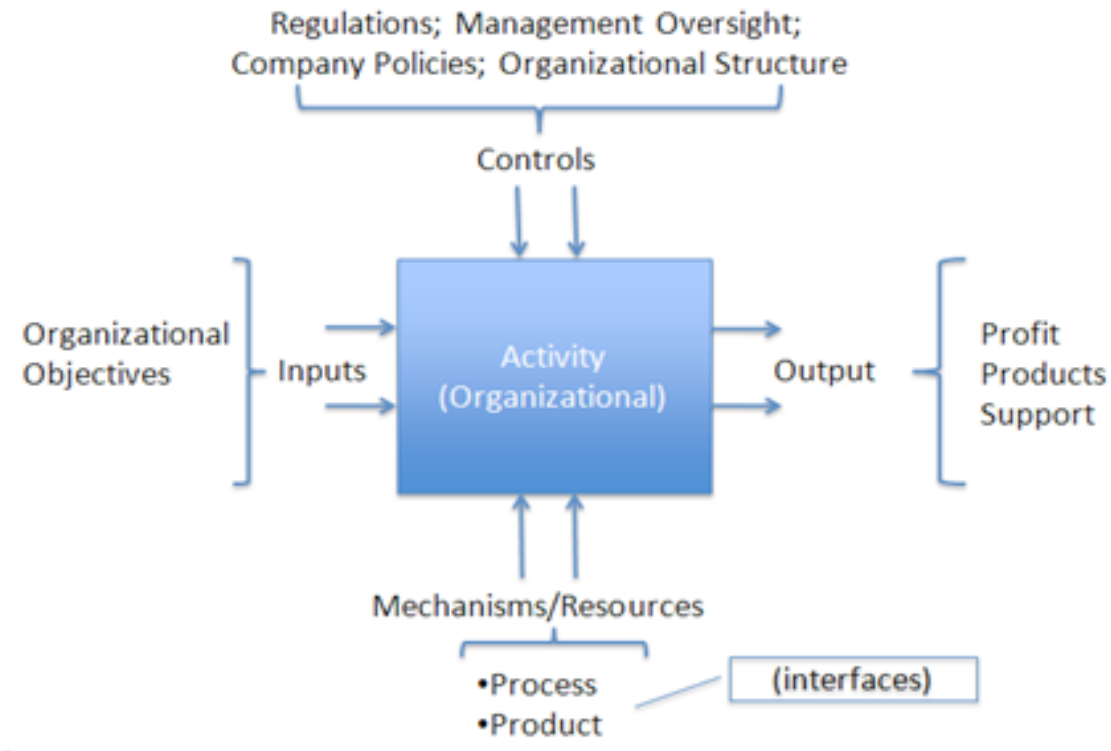
- What methods are used to identify hazards?
- Describe existing manufacturing methods.
- What are the regulatory constraints?
- How is documentation control performed?
- How is organization knowledge maintained over time, i.e., artifacts of prior designs or prior manufacturing methods?
- How are product defects tracked, both during production and in-service? What are the defect rates? Are defect rates known? Are they reliable?

iv) *Product System*

- What method is used to identify requirements?
- What methods are used to identify hazards that the product will encounter in-service? How are such hazards documented and maintained?

- What method is used to identify design requirements? How are materials selected? What environmental factors is the product subject to? How are strength requirements created?
- What design standards exist? What are industry practices for the products? Are any non-standard industry practices used? How were design or manufacturing standards established?
- What methods are used to identify needed toolings?
- How are total in-service times for all sold products known or estimated? How many of the organization products are still in-service?
- What are the testing methods to verify the design? Each manufactured item?
- What quality control and consistency methods are used? Are they effective? What measures support the knowledge?

FIGURE 2. IDENTIFY SYSTEM GRAPHICAL PRESENTATION



b) **AUTHORITIES, RESPONSIBILITIES, AND OUTCOMES**

For the organizational, process, and product domains to be effective, there must be a definition of authorities, responsibilities, and outcomes. That is, *authority* refers to a person or group that controls the overall system and governs change of the system, whereas the *responsible* person or group controls the execution of the system. The authority and responsibility roles exist to produce desired *outcomes*. This step identifies the authorities, responsibilities, and outcomes.

i) *Organizational Domain*

- What is the organizational chart of the organization? Is it up to date?
- What job descriptions exist for each employee? Are they accurate?
- Do all persons know their areas of authority and responsibility and what outcome is expected of them?
- How are individual outcomes measured?
- What is the nature of the authority reporting chain? What level of independence exists as opposed to hierarchal reporting structures?

ii) *Design Domain*

- Who has authority over the design process? *Note:* This is similar to the organizational question, but it looks outward to the personnel, rather than the prior step that looked from people towards outcomes.
- Similarly, who is responsible for each step in the design process?

iii) *Process Domain*

- Who has authority for each process in the organization? *Note:* This is similar to the organizational question, but it looks at the process outward to the personnel, rather than the prior step that looked from people towards processes.
- Similarly, who is responsible for each process in the organization?
- Do the authorities and responsibilities change for different lifecycles of the process supporting a product? For example, is the same person or group responsible for manufacturing as is responsible for customer support of in-service products?
- In terms of outcomes, what processes exist for: marketing, design, production, installation, operation, support, and retirement?

iv) *Product Domain*

- Who has responsibility over each product?
- Who has authority over each product?

- Do the authorities and responsibilities change depending on the product lifecycle, i.e., are the same people responsible for the product during design, production, and in-service?

c) **TASK CATEGORIES**

This step adds more detail to the emerging system description of the organization. The activities that make up an organization are looked at from four perspectives of *operations, administration, supervisory*, and *resources.* While these four perspectives can be considered in the organization, process, and product domains, it is simpler to address the perspectives independent of domains.

i) *Operations Perspective*

- What types of tasks are performed to define the requirements of a product? What types of tasks are performed in designing a product? What types of tasks are performed in manufacturing a product? In delivery/installation of a product? In support of a product? In overhaul or retirement of a product?

- What tasks go into supporting the products and processes, such as accounting, human resources, information technology, and employee training?

- What tasks support business continuity of facilities? Information systems?

ii) *Administrative Perspective*

- What tasks are necessary to maintain regulatory compliance? What tasks to maintain certifications and/or licenses?

- What legal tasks are necessary to support new products? Existing products? Retired products?

- What tasks are necessary for employee timekeeping? Lost work injury reporting?

- What tasks define budgeting?

iii) *Supervisory Perspective*

- What tasks are performed related to supervision, such as employee job reviews and team-building exercises?

- What supports a safety culture, such as a just culture[9]? Is reporting a potential design, process, or product flaw encouraged? If so, how?

- What tasks identify how safety/quality is measured?

- What tasks define how supervisors achieve regulatory compliance?

[9] A just culture means an environment where people are encouraged to report mistakes without fear of reprisal.

iv) *Resource Perspective*

- What tasks are used to define the organization's assets? Credit? Liabilities?
- What tasks are involved in maintaining the accounting systems?
- What tasks are involved in maintaining the information technology systems?
- What tasks are used to manage vendors and suppliers?
- What tasks are used to manage supply inventory?
- What tasks manage orders for future organization products?
- What tasks ensure a sufficient number and quality of employees? What tasks ensure adequate facilities? What tasks ensure adequate tools?

Note: The system description emerging at this point should have a growing amount of detail. The process of creating the system description may have already yielded benefits to the organization in terms of identifying ill-defined areas. Further, the system description process thus far has likely involved many people in the organization contributing needed details.

d) **SYSTEM ANALYSIS**

This system analysis section seeks to identify factors that affect the performance of the system. This is done using an acronym known as SHEL – software, hardware, environment, liveware (people). As was done with task categories, the organization, process, and product domains will not be specifically delineated for sake of simplicity.

i) *Software*

- What organizational policies and procedures exist in the organization? How are they maintained? How are they communicated?
- What templates are used to guide recurring processes?
- What supplier agreements exist?
- What procedures are used to define requirements for new products or product variants? To perform hazard/risk analysis on new product designs?
- What forms of configuration management are used to control manufacturing processes? To control information technology systems?
- What procedures are used to control versions of product manuals?
- What procedures are used to control design specifications?

ii) *Hardware*

- What elements make up the information technology support systems of the organization?
- What facilities are available to the organization and what are the capabilities, i.e., square footage, electrical capacity, size capacity, hazardous material handling?
- What manufacturing tools are required to create products? What spares support the necessary manufacturing tools?
- What raw materials are needed to create the organization's products?
- What defines the interfaces of an organization-produced product with other parts of the system on which it is installed (or operates)?

iii) *Environment*

- Within the organization, how is a just culture maintained—that is, how are employees encouraged to report deficiencies?
- Describe the safety council within your organization.
- How do the legal/litigation aspects of the organization relate or conflict with safety objectives?
- How are workplace rules documented?
- What is the regulatory environment of the organization and its products?
- How is the operating environment wherein the organization products operate factored into design, production, and service?
- How does the economy affect the demand for products?

iv) *Liveware*

- How does the organization attract qualified employees?
- What methods are used to ensure there is sufficient staffing for the organization?
- How are personnel trained to do their jobs? How are they measured in job performance?
- Who are the people who use the products made by the organization?
- Who maintains the products produced by the organization when the product is in-service?
- If applicable, who overhauls/refurbishes products at the end of their lifecycle?

e) **DEFINE WORK DIMENSIONS**

Work dimensions acknowledge the reality that companies exist to make a profit. The work dimensions necessary to make a profit include quality, service, pricing, delivery times, safety, reputation, and others. In some cases, these business objectives promote safety; in other cases the business goals detract from safety.

i) *Organizational Domain*

- How does the organization mitigate against product liability claims?
- How are production rates predicted? How often does production lag behind promised delivery rates?
- What organization procedures are in place to maintain regulatory compliance and reporting?

ii) *Design Domain*

- What methods are used to develop measures of production quality?
- What methods are used to measure customer satisfaction?

iii) *Process Domain*

- What methods are used to develop measures of production quality?
- What methods are used to measure customer satisfaction?

iv) *Product Domain*

- How are safety objectives of a product determined?
- How are customer prices and profit margins determined?
- How are service issues of in-service products determined?
- How are the environmental issues of organization products determined, i.e., for batteries, how are they disposed; for de-icing fluid, how are effects to the environment considered?

f) **DECOMPOSE ACTIVITIES**

This step allows for a detailed description of activities within the organization. Clearly, this list could go on to a level of detail that would be counterproductive. The objective in this step is to create an appropriately detailed outline of activities to facilitate subsequent, deeper analyses.

i) *Organizational Domain*

- What activities are used to maintain the organizational chart?

- What activities are performed to manage the following areas: regulatory compliance, organization assets, information technology resources, facilities, suppliers, intellectual property, and product liability?

- What activities are involved in organization information systems to preserve historical records of the organization?

ii) *Design Domain*

- What activities are used to solicit and develop product design requirements?

- What activities transform requirements into technical designs and how are the designs validated against requirements?

- How activities are used to develop and to measure design quality?

iii) *Process Domain*

- What activities are used to solicit and develop product requirements?

- How are process measures developed to measure quality?

- What activities make up manufacturing of products?

- What activities are necessary to deliver products?

- What activities support in-service products?

- What activities measure the number of active, in-service organization products?

iv) *Product Domain*

- What activities are used to assess how products are actually used and maintained in-service?

- What activities are anticipated to maintain products in-service?

- What activities are performed to train users and maintainers of the product?

- What activities occur in response to failures of the product, i.e., accident and incident investigation?

g) **EXAMINE INTERFACES**

Clearly the activities of an organization are related to each other. This step considers the *interfaces* between activities both *within* and *external* to the organization. In addition to considering interfaces of activities, interfaces of aspects of the SHEL step should also be considered.

i) *Organizational Domain*

- How do actions of the safety council impact policy, procedures, and processes?
- What labor contracts exist? How do labor contracts affect work rules?
- How are non-employee personnel (i.e., vendors, contractors) accounted for in the organization?
- How do financial goals relate to supplier selection?
- How do regulatory requirements affect anonymous reporting and a just culture? Likewise, how do litigation concerns affect anonymous reporting and a just culture?
- If applicable, how do suppliers of products (or labor) affect organization objectives, such as a just culture as well as quality standards?

ii) *Design Domain*

- What product lifecycle data such as service needs, failures, and defects get fed back to the design process?
- How are in-service issues communicated to define design requirements?
- How are these requirements verified in resultant designs?

iii) *Process Domain*

- How do lifecycles of production interface? That is, how are design requirements translated into manufacturing methods? How are design and manufacturing methods used to correct defective and/or broken in-service products?
- How are in-service issues communicated back to design requirements?
- How are manufacturing personnel measured as doing their jobs according to policies created by the organization? That is, how well-aligned is shop floor reality to process design?

iv) *Product Domain*

- How does the organization measure customer usage of its products in-service against the planned in-service usage techniques?
- How are regulatory changes adopted into design changes? How are regulatory changes applied to in-service products (including service bulletins, airworthiness directives, etc.)?

h) **ENVIRONMENTAL IMPACTS**

While the prior step considered interfaces in general, this step looks specifically at how the external environment impacts the functioning of the organization as a system.

i) *Organizational Domain*

- What business continuity plans are in place for manufacturing or office space disasters (i.e., if the manufacturing facility burned down in a fire)?
- What business continuity is in place for information systems?
- How does the organization keep informed of regulatory changes?

ii) *Design Domain*

- How are design requirement changes managed?

iii) *Process Domain*

- How are product requirement changes managed?
- How are manufacturing methods changes managed?
- What is done to protect against dependence on a key, manufacturing tool (or software) becoming obsolete?

iv) *Product Domain*

- How are changing conditions of the environment the products operate in made known to the organization?
- How are supply chain issues needed to manufacture or maintain products assessed?
- How are the organization's products integrated with their host or parallel systems (e.g., if the product is a tire, how is it known it works properly on the landing gear of an Acme 'Rocket' plane)?
- What impact is there on a product's in-service use if the product is retired or upgraded to a newer version?
- What impact is there on any applicable backward compatibility if a product is retired or upgraded to a newer version?

SUMMARY

Performing the eight steps (a-h above) should have created a wealth of notes, artifacts, and raw data. If the process was done in a group environment, there were possibly disagreements that exposed ambiguities not previously known to all parties. The notes taken to this point should be preserved and a system description written that summarizes the organization as a system. Two example work products of this system description procedure for a small Parts Manufacturer Approval (PMA) house that makes rotor shafts and a large multinational organization are provided as Attachments I and II, respectively.

HAZARD IDENTIFICATION

The development of a system description is a prerequisite to an effective, proactive hazard identification process in an organization. This AC closes both by defining a hazard and encouraging the reader to make a list of high-level hazards by providing a list of generic hazard categories.

The D&M SMS Pilot Project Developmental Guidance defines a hazard as: "a condition, occurrence, or circumstance that could lead to or contribute to an undesired event. It is sometimes termed "threat". An "undesired event" can be but is not limited to: injury, illness, or death; damage to or loss of a system, equipment, or property; or detriment to the environment."

a) *Organizational Domain Generic Hazards*

i) Poor definition of authority and responsibilities
ii) Intellectual property compromise
iii) Product liability
iv) Undetected change
v) Regulatory violation
vi) Financial loss

b) *Process Domain Generic Hazards*

i) Changes to methods or procedures
ii) Incomplete process definitions
iii) Changes to supply chain
iv) Manufacturing hazards to personnel (i.e., OSHA type hazards)

c) *Product Domain Generic Hazards*

i) Incorrect product requirements
ii) Product manufacturing defects
iii) Unanticipated failure modes
iv) Products not used or maintained as designed

ATTACHMENT I

Fictitious Example – Small Rotor Shaft Company

The purpose of this section is to show a practical application of the system description process for a small company. This fictitious example considers a small, five-person rotor shaft company, primarily built around a machine shop and a few core products. As the reader progresses through the example, reference should be made to the noted Procedural Document.

Throughout this narrative, certain details may be omitted to express the essence of the process, however, the reader should keep in mind that the process is necessarily an interactive, group exercise. Ideally, the group will have core constituents and invite various members of the organization in to help expand the depth of the expertise at certain stages.

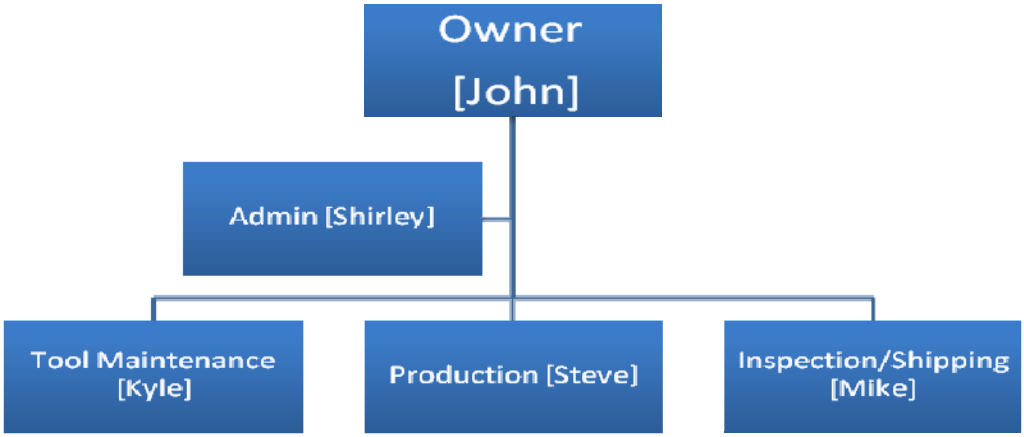
As the system identification process is executed, watch for hazard identification opportunities as the Procedural Document recommends. For any hazard noted in the system description, have a method to add it to the stack of hazards for later consideration. That is, while the process is described linearly, it is fine to jump ahead and move back throughout the process. In this presentation, whenever a discovered hazard is identified it will be enclosed in braces, such as: {HAZ: Defects in supply chain}.

Identify System

The company is looked at from four perspectives: organizational, design, processes, and products.

Item	Hazard (if identified)
Organizational	
The system identified is essentially a machine shop producing rotor shafts under contract to helicopter manufacturers.	{HAZ 1: Machine shop does not know details about design or operational conditions of shafts}
All management are also hands-on workers.	{HAZ 2: Conflicting priorities}
Design	
Designs are documented in fireproof file cabinets, on paper.	
Regulatory constraints defined by customer (helicopter company).	
Process	
Same processes used for many years, as specified by the helicopter company.	
Inspections done by our shop are repeated by the helicopter company upon product delivery.	{HAZ3: May depend on helicopter company to find problems}
Product	

Only new rotor shafts are made, no overhauls. Products limited to what machine shop tooling can handle.



Authorities, Responsibilities, and Outcomes

The organization chart used to identify the system is expanded upon to show authorities and responsibilities within the company.

Item	Hazard (if identified)
Organizational	
President (John) is everyone's boss.	{HAZ4: May lead to personality driven processes}
Design	
John works with helicopter companies to verify designs and setup tooling specifications.	
Process	
Authority for rotor shaft inspections lies with Mike. He reports problems to John, who decides on corrections. Shirley has responsibility to talk to helicopter company for orders and shipping notification.	
Product	
Outcome of a rotor shaft is a mid-process product, which is refined and inspected by helicopter company before installation.	{HAZ5: Failures may be hard to identify – who introduced flaw}
Rotor shafts are expected to last 2,000 hours.	

Task Categories

Task categories are looked at from four areas: operational, administrative, supervisory, and resources. The design, process, and product dimensions are looked at only on the operational area across lifecycle dimensions. Organizationally, the operational and supervisory perspectives were adequately described by the Authorities, Responsibilities, and Outcomes step.

Item	Hazard (if identified)
Organizational	
Administrative functions are handled by Shirley. She does payroll, accounts receivable, accounts payable, subscription renewals, etc.	{HAZ6: When Shirley is sick or on vacation, things may get missed}
Kyle handles computer resources and fixes computers. Backups are done by online backup service.	{HAZ7: Many paper processes and documentation – could be lost if building destroyed}
John ensures there are adequate resources including cash flow for payroll, building leases, utilities contracts, and salary levels.	{HAZ8: Informal process to project adequate cash flow}
Design	
Tasks to define a design include meeting with the helicopter company, creating a statement of work embodied in a contract, affirming non-disclosure, securing design specification documents, and deciding on change control.	
Process	
Company is only concerned with production. Biggest issue is to supplier of raw steel and lead times of 60 days on orders.	{HAZ9: No alternative raw material provider}
Delivery is done by Mike, who needs to crate shaft and get it on truck for delivery.	{HAZ10: Shaft can be damaged during delivery}
Product	
Once helicopter company accepts rotor shaft, our firm has no further obligations. Our contract is written such that the helicopter company takes on full responsibility for the product after delivery.	

System Analysis

Using the SHEL – software, hardware, environment, and liveware – heuristic, the system is analyzed along its organizational, design, process, and product dimensions.

	Item	Hazard (if identified)
	Organizational	
S	Shirley manages people and benefits plans.	
H	Kyle maintains computers and tools on shop floor.	{HAZ11: If lathes change, a new certification is required from helicopter company}
E	Problems in production are reported to John.	{HAZ12: With so few people, cannot have anonymity}
L	Job functions are closely aligned with each person (John, Shirley, Kyle, Steve, Mike).	{HAZ13: Personality driven process, if people were to leave, hard to replace}
	Design	
S	Rotor shaft designs marked by revision. Obsolete versions, when retained, marked as "superseded by."	
H	Large format printers used to print out rotor shaft designs for review and tooling planning.	
E	Just culture in design exists by open-door policy with John if anyone feels a design has flaws.	
L	John is key engineer to maintain and understand designs.	
	Process	
S	Blueprints and spec sheets for shafts stored in fireproof file cabinet in office.	{HAZ14: Original documents guiding production not reviewed often, could lead to practical drift}
H	Shop floor, lathes, and associated tools in working order is critical.	
E	Clean workplace, adequate ventilation, and safety control devices (e.g., hardhats, safety goggles).	
L	Experience of Steve on floor is critical, along with inspections by Mike.	
	Product	
S	FAA form XXX must accompany each delivered shaft.	{HAZ15: Form may become substitute for actual inspection and quality}
H	Produced rotor shaft.	

E	Our company builds shafts to helicopter company specifications – we are not in the loop on actual environment.	{HAZ16: Our knowledge and experience is not fully utilized to see "big picture" problems}
L	Helicopter inspectors who receive shafts from us.	

Work Dimensions

The next step in the system identification process is to look at work dimensions. One way to do so is to organize work dimensions as safety compatible and counter to safety (in the associated table, "✓" is for compatible, "×" is for counter).

	Item	Hazard (if identified)
	Organizational	
✓	Helicopter company annual inspections of facilities and processes for contract renewal.	
×	Minimal workforce for economy limits backup employees.	
	Design and Process	
✓	Quality measures used in the production (by Mike) used to accept or reject shaft.	{HAZ17: Quality measures may not have regular review}
×	Shafts rejected by Mike cost company money.	
	Product	
✓	Minimum defects in delivery.	
×	Desire to stay with one raw material provider.	

Decompose Activities

The work defined thus far has outlined a system. This step draws out specific activities that make up the broader system. This step can be a useful review of the prior steps and will often yield additions to prior steps in the process.

Item	Hazard (if identified)
Organizational	
John reviews contracts, production rates, defect reports, and supervises all employees.	
Shirley processes payroll, accounts receivable, accounts payable, answers phone calls, maintains FAA	

required records.

Design

John meets with helicopter companies to define rotor shaft requirements.

For new or changed shafts, all employees meet to define processes to create and deliver shafts.

Process

Kyle maintains shop tools, John and Shirley's computers.

Steve mounts raw steel on lathe, lathes shafts, cleans/polishes.

Mike inspects shafts, fills out FAA form XXX, provides copies to Shirley along with shipping information, boxes shaft, and arranged truck shipping.

Product

Helicopter company receives and signs off on product.

John is notified, via Shirley, if any rejects by Helicopter company.

Examine Interfaces

Like decomposing activities, interfaces provide another retrospective opportunity.

Item	Hazard (if identified)
Organizational	

John works with helicopter companies, gets accounting information from Shirley, and oversees production quality received from Mike.

Shirley gets records of shipping and production form FAA XXX from Mike; Kyle fixes computer issues for Shirley and makes sure online backups work.

Kyle fixes Shirley's computer when it breaks and advises John when tooling is in need of replacement.

Design

Problems on assembly line are related to John, who considers modifying process design.

Process and Product

Steve advises Kyle when shop equipment needs repair or calibration; advises Mike when a shaft is ready for inspection.

Mike works with shipping company to send shafts; crate company to keep supply of crates and shipping materials; provides Shirley with records of shipping.

Environmental Impacts

Item	Hazard (if identified)
Organizational	
Each employee has irreplaceable knowledge with little duplication of skill.	
Process	
Location of filing cabinet with original designs (blueprints) is far from shop floor, so difficult to inspect.	{HAZ18: Practical drift in production}
Designs don't change often, but when they do it takes awhile to get up to speed.	
Product	
Shaft failure in operations is a catastrophic event.	{HAZ19: Chain of authority through helicopter company may obscure how critical our role is}

Hazard Identification

The system analysis should have spawned numerous opportunities to identify hazards in the system, again broken down by organizational, design, process, and product. Within this example, the process produced many hazards, but still only a subset of what an actual execution of the process would yield. The hazards identified while conducting the system description should be collected and used as a starting point for a dedicated hazard analysis.

Organizational
Machine shop does not know design or operational details of shaft usage.
Small company leads to conflicting priorities of Management (John).
Personality driven processes.
When Shirley is sick or on vacation, things may get missed.
Paper documentation all in one place.
Informal process to project adequate cash flow.

If lathe changes, a new certification is required from helicopter company.

With so few people, cannot have anonymity.

Personality driven process – if people were to leave, hard to replace.

Design

Quality measures may not have regular review.

Process

Helicopter company is relied upon to ultimately identify defects.

No alternative supplier of raw materials.

Shaft damage during delivery.

Original documents (blueprints) guiding production not reviewed often.

Quality measures may not have regular review.

Practical drift in production.

Product

Failures in shaft may be hard to identify in our company or helicopter company.

FAA Form XXX may be substitute for actual intent – quality, defect free shaft.

Our knowledge and experience is not fully utilized to see “big picture” problems.

Chain of authority through helicopter company may obscure how critical our role is.

Conclusion

The system description of the company is the foundation of a safety management system. It should become clear by the time the analysis is executed that the system analysis herein is a macro view of the company. What follow the macro view are numerous micro views of many supporting processes: a similar analysis procedure can and should be executed for each process within the company.

ATTACHMENT II

Fictitious Example – Aircraft Design and Manufacturer

The purpose of this attachment is to show a practical application of the system description process using a fictitious example of an aircraft design and manufacturing organization.

Throughout this narrative, certain details may be omitted to express the essence of the process, however, the reader should keep in mind that the process is necessarily an interactive, group exercise. Ideally, the group will have core constituents and invite various members of the organization in to help expand the depth of the expertise at certain stages.

As the system identification process is executed, watch for hazard identification opportunities as the Procedural Document recommends. For any hazard noted in the system description, have a method to add it to the stack of hazards for later consideration. That is, while the process is described linearly, it is fine to jump ahead and move back throughout the process. In this presentation, whenever a discovered hazard is identified it will be enclosed in braces, such as: {HAZ: Defects in supply chain}.

Identify System

The company is looked at from four perspectives: organizational, design, processes, and products. The assessment team decided the process and product domains would be analyzed together in this first step.

Item	Hazard (if identified)
Organizational	
The system identified is a multinational aircraft design and manufacturing organization.	{HAZ1: Cultural and linguistic differences interpreting organizational information}
A multinational company that has grown by acquiring other aircraft manufacturing companies.	{HAZ2: Conflicting procedures}

Note: The complete picture of the organization would have the subordinate organizations repeating the process described herein.

The design aspect includes support of retired designs from the legacies of the acquired companies, modification of designs for new variants and wholly new designs for emerging markets.

Note: The structure of the varying companies is represented by a high-level organization chart (high-level organizational chart would be inserted here).

The differing corporate entities often produce sub-assemblies of an aircraft in production.	{HAZ3: Defects introduced in moving sub-assemblies to final assembly}

The outcome of the company is to produce safe, reliable aircraft that generate a profit not only for the

parent manufacturing company but also for the operator of the aircraft.

The parent company also seeks to successfully identify emerging markets for new aircraft designs.

Design

Hazards identified through design reviews, fault tree analysis, failure mode effects analysis.

Organizational knowledge maintained in corporate knowledge portal.

Process and Product

Parent and subordinate companies have developed a rich variety of proven methods to identify requirements, develop designs, conduct hazard analysis, supplier source selection, internal testing methods and approaches to certification conforming to various countries.

Methods have developed in accordance with standards such as AS9100, SAE standards, and 14 CFR Part 25 to name a few (cross references to these existing methods would be inserted here).

Authorities, Responsibilities, and Outcomes

The high-level organization chart used to identify the system is either reused or expanded upon to show authority and responsibility within the company. The assessment team again decides to combine process and product domains in this step.

Item	Hazard (if identified)
Organizational	
Company consists of multiple, somewhat autonomous subsidiaries.	{HAZ4: Ill-defined authority across subsidiary boundaries}
The change management process of the parent company includes management of new acquisitions and identification of change in existing subsidiaries.	
Design	
Authority over design process with Chief of Engineering.	
Responsibility for design process lies with Engineering Department.	
Process and Product	
Accountability is by product line, which is to say each aircraft has an Accountable Executive (AE) assigned.	
The AE develops a team of leaders, each responsible for varying facets of the aircraft, be it	{HAZ5: Supervision, check/balance of AE}

in production or in operational support.

For each aircraft, an organizational chart starting at the AE and descending through the team leaders is maintained and has a change management process.	{HAZ6: Loss of intellectual inventory when personnel retire or attrition}

Task Categories

Task categories are looked at from four areas: operational, administrative, supervisory, and resources. The design, process, and product dimensions are combined in this example with focus only on the operational area across lifecycle dimensions. Organizationally, the operational and supervisory perspectives were adequately described by the Authorities, Responsibilities, and Outcomes step.

Item	Hazard (if identified)
Organizational	
The administrative dimension includes typical corporate functions such as human resources, marketing, accounting, etc.	
The resource dimension include items such as adequate lines of credit and cash reserves to operate the company, information technology systems, customer support systems, and facilities management.	{HAZ7: Business continuity of information technology}
Design, Process, and Product	
The requirements lifecycle contains methods for market analysis and iterative requirements identification methods leading to design specifications.	{HAZ8: Scope creep in requirements; requirements omissions}
The design lifecycle includes CAD design techniques, wind tunnel analysis or simulations thereof, electronic simulations of human factors, creation of specifications for flight training simulators, and type certification documentation.	{HAZ9: Incompatible software versions across supply chain}
When the aircraft is in production, task categories include management of logistics for sub-assembly integration, supply chain management, manufacturing automation setup, and measurement of production rate and quality.	{HAZ10: Shortage of supply can stop assembly line} {HAZ11: Business continuity of shop floor automation logic (may differ from other information technology systems)}

The delivery lifecycle includes certification of each aircraft produced, operational and maintenance manuals, and end user training.	{HAZ12: Version management}
The operations lifecycle requires task categories of product support and priority escalation of key issues, replacement parts, and participation by the company in use case analyses of aircraft operators (customers) to verify such use cases were considered during aircraft design, and participation in accident/incident investigation.	{HAZ13: Operator is planning on flying into gravel runway} {HAZ14: New hazards discovered may not feed back to full product lifecycle, i.e., requirements}

When the company retires the product, methods exist to maintain adequate replacement parts for in-service aircraft.

System Analysis

Using the SHEL – software, hardware, environment and liveware – heuristic, the system is analyzed along its organizational, design, process, and product dimensions.

	Item	Hazard (if identified)
	Organizational	
S	Employee job descriptions and goals as well as a company repository of policies and procedures maintained on the corporate intranet in addition to templates for engineering and safety processes.	{HAZ15: Version control across geographically disparate companies; different languages of employees (localization)}
H	The hardware perspective includes information technology support for a document management system, website and telecommunication capabilities, leases on facilities and equipment, and maintenance of manufacturing tooling.	{HAZ16: Cyber attack} {HAZ17: Natural disaster; terrorism} {HAZ18: Obsolete tools}
E	Maintenance of a just culture and anonymous safety reporting programs, a safety council, and legal agreements with suppliers and airframe organizations.	
L	The liveware component contains the employee training for job functions and the promotion of the safety culture.	{HAZ19: New acquisitions may have inherent distrust of new parent}
	Design	

S	Electronic repositories of procedures to perform requirements analysis, design, and verification.	
H	Engineering work stations, networked computing environment, electronic whiteboards.	
E	Safety council reviews designs. Accidents and incidents in operations are compared to designs to identify issues for correction.	
L	Adequate staffing of employees and proper training.	
	Process	
S	Electronic repositories of procedures to perform testing, production, quality measures, installation, and field support.	{HAZ20: Intranet documents not available in all necessary areas due to security}
H	Production and office facilities along with shop tools and materials inventory.	
E	Clean workplace, adequate ventilation, and safety control devices (hardhats, safety goggles, etc.).	
L	Adequate staffing of employees and proper training.	
	Product	
S	Manuals for the end user, limitations and maintenance.	{HAZ21: Design features may make certain maintenance functions overly complex}
H	Raw materials supply as well as the need for simulators for aircrew training.	
E	Atmospheric operating environments for the aircraft as well as the operator use cases for the aircraft in practice.	{HAZ22: Operator use cases may not match design}
L	How the product is used and maintained in operations as well as practical drift from designed operations and actual operations. Passenger comfort issues within the control of the manufacturer are also part of the system.	{HAZ23: Cabin configuration variants impact on emergency egress}

Work Dimensions

The next step in the system identification process is to look at work dimensions. One way to do so is to organize work dimensions as safety compatible and counter to safety (in the associated table, "✓" is for compatible, "✗" is for counter).

Item	Hazard (if identified)
Organizational	

✓	Safety council and regulatory compliance objectives.	{HAZ24: Active engagement of safety council over time}
×	Short-term profit and production goals.	
×✓	Organization of the company by subsidiary can be both safety compatible through specialization and expertise, but can also be safety counter if the subsidiaries fail to effectively communicate safety or productivity issues.	
	Design	
✓	Design features emphasize state-of-the-art safety features to compete with other companies.	
×	Designs must be price competitive, which may conflict with safety goals.	
	Process	
✓	Quality measures used in the production processes and testing for certification.	{HAZ25: Wrong measures; unused measures} {HAZ26: Design to certification rather than to (higher) safety standard}
×	Trying to avoid rework or use of disposable materials as well as overworking employees.	
	Product	
✓	Minimum defects in delivery as well a rigorous certification process.	
×	Overuse of lightweight materials or low-cost suppliers with insufficient controls on quality.	

Decompose Activities

The work defined thus far has outlined a system. This step draws out specific activities that make up the broader system. This step can be a useful review of the prior steps and will often yield additions to prior steps in the process.

Item	Hazard (if identified)
Organizational	
Maintenance of the company organizational chart, annual benefits communication, supplier visits, industry conferences, employee performance reviews, monthly accounting and reporting, business continuity testing, and information technology software and hardware upgrades	{HAZ27: Non-competitive benefits may cause attrition of key personnel}
Design	
All design components required to have quality measures	
Design improvements solicited from customer feedback and review of industry trends	
Process	
Requirement meetings, creation of CAD drawings, simulations, FMEA analysis, wind tunnel testing, tooling automation setup, time-tracking, training, and assembly of sub-assemblies	{HAZ28: External component supplier may limit FMEA analysis depth}
Product	
Production of operator and maintenance manuals, advertising of new products, phone center activity to receive and process inbound communications, responses to critical safety concerns, accident investigation participation, and inventory counts	{HAZ29: Escalation of safety issues may not be flagged}

Examine Interfaces

Like decomposing activities, interfaces provide another retrospective opportunity.

Item	Hazard (if identified)
Organizational	
The just culture may be taken advantage of by certain employee personality types.	
Differing compensation between subsidiaries could cause intra-company transfers and associated retraining costs.	
Information technology downtime effects nearly all processes of the company, regulatory violations can shut down production, and supplier defects can compromise product integrity.	{HAZ30: Anti-virus software slows down computers; system maintenance causes downtimes at key production milestones}
Design	
All flight test defects routed through Engineering Department for design review	
Warranty department and customer service flow through Engineering Department	
Process and Product	
How the aircraft operators choose to operate the aircraft – operational use cases may not be those anticipated in design (as mentioned earlier)	
Operating manuals and specifications may not match the current revision of the production aircraft	
Design and production changes require updates to hazard/risk analysis	{HAZ31: Workflow for production changes may be incomplete}
Defects discovered in operations may require corrective actions such as airworthiness directives	

Environmental Impacts

Item	Hazard (if identified)
Organizational	
Intellectual sabotage, patent infringement, natural disasters destroying production facilities, information technology systems failures, employee turnover, economic downturns, accidents in production or in operations, and	{HAZ32: Lack of involvement in regulatory change process in differing jurisdictions}

regulatory changes to airworthiness requirements

Design
All design changes go through a design review process.

Process
Changes to requirements, tooling failures in production, obsolescence of necessary tooling, and practical drift in production processes

Product	
Actual environments differing from the design environment, undetected product flaws entering the operational environment, component incompatibilities	{HAZ33: Component failures may be reported to component manufacturer, not to aircraft manufacturer}
Simulator behaviors do not match the actual characteristics of the aircraft	{HAZ34: Simulator trained techniques may not match anticipated design}

Hazard Identification

The system analysis should have spawned numerous opportunities to identify hazards in the system, again broken down by organizational, design, process. and product. Within this example, the process produced many hazards, but still only a subset of what an actual execution of the process would yield. The list that follows is a compilation of the hazards identified and should be used as a starting point for a hazard identification process.

Organizational
Cultural and linguistic differences interpreting organizational information
Conflicting procedures
Defects introduced in moving sub-assemblies to final assembly
Ill-defined authority across subsidiary boundaries
Business continuity of information technology
Version control across geographically disparate companies; different languages of employees (localization)
Cyber attack
Obsolete tools

Natural disaster; terrorism

New acquisitions may have inherent distrust of new parent

Active engagement of safety council over time

Non-competitive benefits may cause attrition of key personnel

Anti-virus software slows down computers; system maintenance causes downtimes at key production milestones

Lack of involvement in regulatory change process in differing jurisdictions

Design

Scope creep in requirements; requirements omissions

Incompatible software versions across supply chain

Shortage of supply can stop assembly line

Business continuity of shop floor automation logic (may differ from other information technology systems)

Version management

Operator is planning on flying into gravel runway

New hazards discovered may not feed back to full product lifecycle, i.e., requirements

Process

Supervision, check/balance of Accountable Executive

Loss of intellectual inventory when personnel retire or attrition

Scope creep in requirements; requirements omissions

Incompatible software versions across supply chain

Shortage of supply can stop assembly line

Business continuity of shop floor automation logic (may differ from other information technology systems)

Version management

Operator is planning on flying into gravel runway

Intranet documents not available in all necessary areas due to security

Wrong measures; unused measures

Design to certification rather than to (higher) safety standard

External component supplier may limit Failure Modes and Effects Analysis depth

Workflow for production changes may be incomplete

New hazards discovered may not feed back to full product lifecycle, i.e., requirements

Product

Supervision, check/balance of Accountable Executive

Loss of intellectual inventory when personnel retire or attrition

Scope creep in requirements; requirements omissions

Incompatible software versions across supply chain

Shortage of supply can stop assembly line

Business continuity of shop floor automation logic (may differ from other information technology systems)

Version management

Operator is planning on flying into gravel runway

New hazards discovered may not feed back to full product lifecycle, i.e., requirements

Design features may make certain maintenance functions overly complex

Operator use cases may not match design

Cabin configuration variants impact on emergency egress

Escalation of safety issues may not be flagged

Workflow for production changes may be incomplete

Component failures may be reported to component manufacturer, not to aircraft manufacturer

Simulator trained techniques may not match anticipated design

Conclusion

The system description of the company is the foundation of a safety management system. It should become clear by the time the analysis is executed that the system analysis herein is a macro view of the company. What follow the macro view are numerous micro views of many supporting processes: a similar analysis procedure can and should be executed for each process within the company.